Fundmental — أساسيات

* العمليات التي يقوم بها الكمبيوتر

[1] Hardware

وحدات ادخال	وحدات اخراج	معالجة	تخزين
لوحة المفاتيح	الشاشة	Rom	Hard disk
الماوس	الطابعة	RAM	DVD
الماسح الضوئي	السماعات	Processor المعالج	USB
		BIOS	CD

[2] Software

Operating system نظام التشغيل	Application التطبيقات	برامج التشغيل
windows	Access	← برنامج تشغيل الطابعة
mac	GTA	← برنامج تشغيل الماوس
linux		
Android		

ROM → Read only Memory

ذاكرة تقوم بتخزين البرامج الأساسية وبرامج التشغيل ولا يمكن تعديلها لانها تحتوى على معلومات من الشركة المصنعة ولا يمكن للجهاز أن يعمل بدونها وتحتفظ بالبيانات ولا تتأثر بانقطاع التيار الكهربى.

RAM → Random access Memory ذاكرة عشوائية

تقوم بمعالجة البيانات التي يتم استخدامها في الوقت الحالى ولكنها تتأثر بانقطاع التيار الكهربى ← اسرع من ROM

BIOS → Basic Input output system نظام الادخال والاخراج

هو المسئول عن قراءة جميع مكونات الجهاز عند بداية فتحه ويحتوى على معلومات لا يمكن حذفها ولكن يمكن تحديثها لقراءة اشياء جديدة.

* الكيسه [CPU] تتكون من جزئين علوي وسفلي

North Bridge ⇒ - Graphic card كارت الشاشة
- Processor
- RAM

South Bridge ⇒ - BIOS - USB - Audio - Harddisk - DVD - CD
- LAN كارت النت

* أنواع الكمبيوترات الشخصية → Personal Computers

[1] الحواسب الصغيرة — PC - laptop
[2] الحواسب المتوسطة — Super minis
[3] الحواسب الكبيرة — Main frames
[4] الحواسب العملاقة — Super Computer

* End devices [Computer - mobile -----]

It is the main Component because it is a source of network Application.

هي المكون الاساسي لانها تقدم التطبيقات.

→ network application :

It is a service that can be done by remote devices.

** تعريف اتصالات البيانات :

عمليـــة تبادل ونقل البيانات الرقمية بيـــن جهازيـــن أو أكثر مـــن خلال وسط سلكيـــة او لاسلكيـــة .

** المعايير الاساسيـــة لجـــودة اتصالات البيانات :

1 التوصيـــل :- Delivery

القدرة على توصيـــل المعلومات كما هي .

2 الدقـــة :- Accuracy

القدرة على توصيـــل المعلومات بدقـــة

3 التوقيـــت :- Time Line

سرعة توصيـــل البيانات في الوقت المحدد ولو ماوصلش هيحدث delay

** عناصـــر نظام اتصال البيانـــات :-

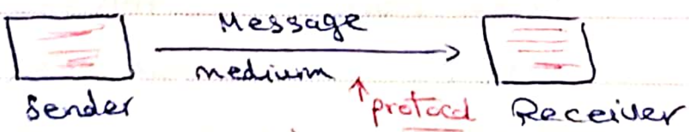
① الرسالـــة Message :- البيانات التي سيتم ارسالها [mp3, video ...]

② الراسـل Sender :- الجهاز القائم بارسال الرسالـــة [PC-Mobil]

③ المستقبل Receiver :- الجهاز المستقبل للرسالـــة [PC-Mobil]

④ وسط الرسالة Transmission medium :- العنصر المادي المستخدم لارسال الرسالة ويكون كابلات سلكيـــة او لاسلكيـــة .

⑤ البروتوكول protocol :- مجموعة القواعد Rules التي تحكم عملية الارسال



تعريف الشبكة ← هو ربط أجهزة الحاسب ببعضها البعض عن طريق ربطها فوق على بطاقة شبكة تحول البيانات الى Binary

→ Ip Network definition:

It is group of Components that are connected together to provide aservice [application]

---

* Importance of Network   أهمية الشبكة

1. Easy sharing of files, Information and data Base
2. Easy sharing of expensive devices [printer]
3. Security of Information
4. Voice - video - taste - smell - touch
5. Make aBackup   عمل نسخ احتياطي بشكل تلقائي
6. IoT → internet of things

---

* تطبيقات الشبكات

تعتمد على distributed processing المعالجة الموزعة

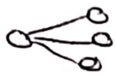
① شبكات الحاسوب العادية
② البريد الالكتروني electronic email
③ الاتصال الصوتي Voice Mail
④ نقل الأموال من البنوك ATM
⑤ المؤتمرات عن بعد . Tele Conferencing



ملحوظة
① كل جهاز على الشبكة يسمى node .
② الجهاز الواحد قد يكون كمبيوتر او طابعة او ماسح ضوئي
③ وسط الاتصال قد يكون سلكياً او لاسلكياً .

* Line Configuration   اسلوب خط الاتصال

[1] point to point → بين جهازين 

[2] Multi point → بين عدة اجهزه 

* type of Transmission :-   اسلوب الارسال

[1] الاسلوب البسيط Simplex direction :- Transmission in 1 direction

هو قيام أحد الاجهزة بالاستقبال فقط مثل [التليفزيون - الراديو]

[2] اسلوب الارسال والاستقبال النصفي Half duplex :-

Transmission in two directions but not at the same time.

قيام الاجهزه بالاستقبال والارسال ولكن ليس في نفس الوقت [هواتف الشرطة]

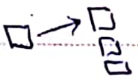
[3] اسلوب الارسال الكلى Full duplex :-

Transmission in two directions In the same time

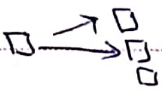
يمكن للجهاز الارسال والاستقبال في نفس الوقت مثل [المحمول]

* Casting types :-

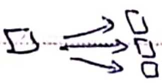
[1] unicast :- means send data for one of all receivers

 تعني ارسال الداتا لمستقبل واحد

[2] Multicast :- means send data for some receivers

 تعني ارسال الداتا لمجموعة مستقبلين

[3] Broadcast :- means send data for all receivers

 تعني ارسال الداتا لكل المستقبلين

* أنواع الشبكات من حيث حق الوصول الى خدمات الشبكة :-

1. الانترنت :- هي الشبكة العالمية للانترنت وتستخدم بروتوكول الانترنت IP .
2. الانترانت :- شبكة داخلية بين فروع الشركة بين شبكة محلية ويتم الربط بين هذه الشبكة عن طريق الروتر مثل [شركة اوراسكوم] .
3. الاكسترانت :- مجموعة شبكات ايرانت يتم توصيلها على مستوى العالم دون المساس بخصوصية الانترنت .

* المعايير الأساسية للشبكات :-

أولاً :- الأداء Performance :- سرعة الشبكة تعتمد على

1. عدد المستخدمين ← قد تسبب زيادة users لسقوط الشبكة [الثانوية]
2. نوع وسط نقل البيانات Transmission medium .
3. الموارد المادية Hardware
4. البرمجيات Application

ثانياً :- الموثوقية Reliability :- دقة وصول البيانات تعتمد على

1. تكرار خروج الشبكة من الخدمة [العطل]
2. الزمن المطلوب لعودة الشبكة .

ثالثاً :- الحماية Security :-

1. الحماية من الفيروسات
2. الحماية من المستخدمين غير الشرعيين unauthorized user وهم الهاكر Hackers .

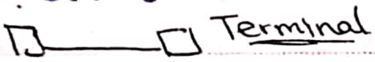
* الخادم server :- أجهزة حاسب لها قدرات فائقة [تخزين -] ويقدم الخدمة
* العميل client :- اجهزة حاسب شخصية تحصل على الخدمات من السرفر server
* مصادر الشبكة Resources :- الملفات والأجهزة المستخدمة .

Network types أنواع الشبكات

① حسب المكونات

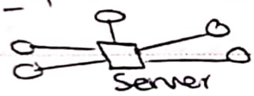
1 peer to peer :- شبكة النظير [الند بالند]

← كل الوحدات متماثلة وليس هناك سرفر بعينها ويمكن لأى جهاز موجود بالشبكة أن يستجيب من البيانات على جهاز اخر



2 Server Based Network: شبكة الخادم والعميل

هناك سرفر يقوم بتقديم الخدمة للعميل domain client حيث ان الخادم يتحكم في الشبكة ويقوم بتجزيء برامج نظم التشغيل.



② حسب البعد



1 LAN [Local area network] الشبكة المحلية

group of components that connected together to provide a service in local area network

← مجموعة اجهزة تتصل مع بعضها لمسافة محدودة [100 m] وفي الغالب يتم استخدام كابلات ويتم استخدام هنا الوسائط الصغيرة.

2 MAN [metropolitan area network] شبكة المدن

group of LANS in the same city between service provider

← مجموعة LANS متصلة في مساحة أكبر كمدينة مثلاً وتصل لمساحة [10 km]

يمكن استخدام الكابلات او توصيل لاسلكي مثل توصيل فروع [QNB]

3 WAN [wide area network] شبكة واسعة النطاق

groups of LANS between cities between Service Provider

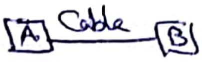
← توصيل LANS على مستوى العالم سلكياً او لاسلكياً

← لو عندي شبكة داخلية تبقا LAN لو خرجت بره تبقا WAN

- The biggest public wan → Internet
- The biggest private wan → Orange

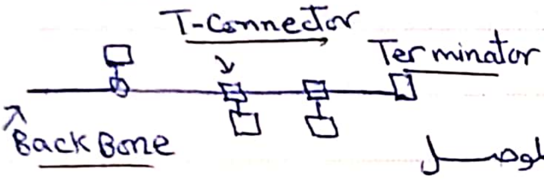
→ Network Topologies:- طرق ربط الشبكات

[1] point to point topology:-



توصيل بين طرفين فقط

[2] Bus Topology:- الشكل الخطي



عبارة عن خط رئيسي يسمى Bus يتم من خلاله
تبادل المعلومات حيث انه خط رئيسي يوصل للاجهزة .
← يتم نقل البيانات بين جهازين عن طريق استخدام الموصل
T-connector ويتم وضع في نهاية الشبكة جهاز يسمى Terminator والكابل
الرئيسي الذي يربط جميع الاجهزه يسمى BackBone

طريقة العمل:- all devices receive the signal .

ترسل البيانات على الشبكة على هيئة اشارات كهربية Signals الى كل
الكمبيوترات الموصلة ويتم قبول المعلومات من قبل الكمبيوتر الذي له نفس المعلومات
ولكن هناك مشكلة انه اذا قام جهازين بالارسال في نفس الوقت يحدث
تداخل Collision لذلك يجب ان كل جهاز ينتظر الاخر حتى يقوم بالارسال مما يؤدي
الى تباطؤ الشبكة ويتم وضع Terminator والذي يقوم بامتصاص الاشارة

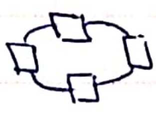
المميزات:-

قليلة التكلفة لوجود ناقل واحد للبيانات للربط بين الاجهزة .

العيوب:-

① يحتاج الى مسافة كبيرة لصعوبة الوصول الى الكثير
② الشبكة تتعطل في حالة وجود عطل في كبل الشبكة

[3] Ring Topology:- الشبكة الحلقية



الشبكة تكون مبنيه على شكل حلقة و البيانات تنتقل من جهاز ع للذي
يليه Token ring معناها دائرة الحلقات أي أن كل جهاز يقوم بالارسال عن
طريق استقلال الشبكة وهذا البروتوكول يوقف كل المراسلات الى حين ينتهي
المرسل من الارسال وهو Token protocol .

المميزات :-

① سهولة ادارتها

② قلة التكلفة لوجود خط رئيسي في كل حلقة .

العيوب :- تتعطل اذا حدث عطل او قطع كابل حيث ان كل جهاز يكون جزء من الشبكة .

[4] Mesh Topology:



تسمى بالمعقدة لان الشبكة تتكون عن طريق ان كل جهاز يتصل بالاخر بطريقة مباشرة عن طريق كابل .

المميزات :- اذا حدث عطل في مسار واحد لا تتأثر الشبكة نظراً لوجود أكثر من حل وأن كل جهاز متصل بجهاز اخر بطريقة مباشرة

العيوب :-

① مرتفعة التكلفة لكثرة الكابلات

② يصعب اكتشاف الاخطاء وتصليحها لكثرة الكابلات

طريقة حساب عدد الكابلات :- no of Cables $= \frac{n(n-1)}{2}$

[5] Star Topology:



Centeralized device [Router, Switch]

Switch - HuB

تتوزع كل شبكة من مجموعة اجهزه حول جهاز مركزي ويكون

المميزات :-

① كل الاجهزه تستطيع العمل في نفس الوقت

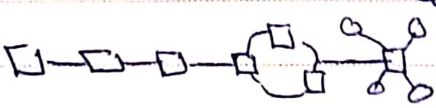
② لا يؤثر حاسوب بالشبكة على عملها

العيوب :- ① تكلفتها عالية نظراً لاتصال كل الاجهزه بالجهاز المركزي

② اذا حدث عطل في الجهاز المركزي تتعطل الشبكة بالكامل

[6] Hybrid Topology:

تربط بين شبكات من انواع مختلفة .



* Access Method   طريقة مرور الداتا

- data in medium like trains in railways
- Access Method types:-

→ CSMA /CD [carrier sense multiple access with collision detection]

ان الجهاز ينتظر الاخرين يقوموا بالارسال وبعد ذلك يقوم هو بالارسال لان اذا قام الاثنين بالارسال في نفس الوقت هيحصل Colloision فكل جهاز ينتظر وقت عشوائي.

→ Token passing

عبارة عن ان يكون هناك اشارة signal اللي يلحقها يستخدمها

ليه الطريقة المستخدمة هي CSMA/CD بالرغم من انها تسبب Colloision ؟

[1] Token pass بطيئة بالنسبة لـ CSMA

[2] في حالة استخدام Star topology يعمل على تنظيم الحركة.

Cables - Connectors الموصلات

Connection
- Cables الكابلات
  - Fiber
  - النحاسية copper Cable
    - Twisted pair
      - FSTP
      - STP
      - UTP
    - Coaxial Cable
- Wireless اللاسلكي
  - Bluetooth
  - wi-fi
  - Infra red تحت الحمراء

⇒ Wireless Communication :- تقنيات الشبكات اللاسلكية

1 Infra red الاشعة تحت الحمراء :-

من اقدم التقنيات التي كانت مستخدمة وانتشرت بشكل محدود لانها كانت تغطي مساحات صغيرة فقط

2 WIFI :-

الاسرع انتشاراً من تمكن من الاتصال اللاسلكي وغالباً ماتكون في المناطق العامة سرعتها اقل من سرعة الاتصال عن طريق كابل DSL ولكنها كافية للعمل

3 Bluetooth البلوتوث

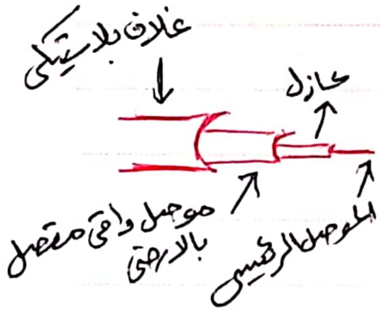
اتصال لاسلكي بين الاجهزه يغطي مساحة محدودة

← الهدف هو عمل شبكة داخلية صغيرة دون الحاجة لتوصيل كابلات

⇒ Cables :-

الكابل هو الوسط المادى للتوصيل بين الاجهزه لنقل المعلومات

[1] Coaxial cable   [الكابل متحد المحور]



هو الكابل المستخدم فى الدش وكان مستخدم قديماً للكمبيوتر
. سمى بالكابل متحد المحور لانه يحتوى على ٢ من الموصلات موصل
أساسى وموصل متصل بالارض مجدول شبكياً [Braided]
ويفصل بينهما طبقة عازله حيث ان هذه الشبكة
المعدنية الواقية متصلة بالارض earth فلا يؤثر للتشويش
من الخارج على السلك المحورى . Noise

← يوجد بها موصل BNC لنهاية اطراف الكابل و BNC-T وصله مشترك

← دائماً تستخدم فى Bus Topology

الكابل المحورى ينقسم الى نوعين

Thin	Thick
- 10 Base 2	- 10 Base 5
- يستخدم فى الشبكات الصغيره	- يستخدم فى الشبكات الكبيرة
- التكلفة قليلة	- التكلفه كبيرة
- السرعه 10 mbps	- السرعه 10 mbps
- المسافة 185 m	- المسافة 500 m

[2] Twisted pair cable الكيبلات المجدولة

- هي الأكثر استخداماً
- يشبه سلك الهاتف ولكن يتكون من ٨ اسلاك داخلية بينما سلك الهاتف يتكون من سلكين
- يسمى Twisted لانه يتكون من ٤ أزواج [4 pair]

[1] UTP → unshielded twisted pair أزواج غير محمية

- تتكون من ٨ أزواج ولكن ليس عليهم داع خاص للحماية من noise
- تقسم مؤسسة TIA / EIA معايير هذه الكابلات على Cat 1 و Cat 4
- عند وجود سلك نت بجوار سلك الكهرباء تحدث مشكلة في الاستقبال لانه يتولد حول سلك الكهرباء مجال كهرومغناطيسي electromagnetic field فيسبب تشويه الكهرباء ويمكن معرفة الخطأ عن طريق المقارنة بين الاصل والصورة ويرسلها ١٦ مرة — محمي سلك كهربي
- الحل لهذه المشكلة

[1] المسافة بينهم تكون ٦٠ سم distance between them 60 cm

[2] STP

[2] STP → Shielded twisted pair أزواج محمية

في هذه الكابلات يتم تغليف الاسلاك تغليفاً منفصلاً أو مجمعاً وهذا يعمل على العزل الكهرومغناطيسي للسلك مما يعطيه بعض المميزات منها

[1] اقل عرضه للتداخل الكهرومغناطيسي
[EMI] → Immune against Interference [EMI] electromagnetic Interference

[2] تستطيع دعم الارسال لمسافات بعيدة
[3] قد توفر سرعات أكبر

← من أساليب العزل الكهرومغناطيسي 2-

1 U/FTP تغليف فردي

تغليف فردي من رقائق الألمونيوم لكل زوج [برتقالي + ابيض برتقالي] وهذا التغليف يحمي الكابل من Noise الخارجي من التشويش القادم من الأزواج المجاورة.

2 F/UTP تغليف كلي

يحمي الكابل لجميع الأزواج مرة واحدة للحماية من الخارج

3 S/FTP تغليف فردي وكلي

تغليف الكابل لجميع الأزواج ككل ولكل زوجين معاً مما يعمل على الحماية من التشويش الداخلي بين الأزواج ومن التشويش الخارجي .

ملحوظة

→ [UTP - STP] use RJ-45 [Registered twisted pair] connector

→ Maximum segment length for all types twisted pair is 100 meter

← يتم استقبال الداتا في UTP و STP على هيئة شحنات كهربية

1 → 5 V (Binary) 0 → 0 V (Binary)

← أنواع كروت LAN

→ Ethernet → 10 Mbps = 10 mega bit per second

→ Fast Ethernet → 100 Mbps

→ Giga Ethernet → 1 G → Mbps = 1024 Mbps

→ Ten Ethernet → 10 Gbps = 1024 x10 Mbps

→ Hundered Ethernet → 100 Gbps

→ wireless Ethernet [wifi] → 1 Gbps

مسافة LAN يمكن تغطيتها 100 m ولو مسافة أكبر نستخدم WAN

معايير تقسيم TIA / EIA لكابلات Categories of UTp

CAT 1 الفئة الأولى :-

يستخدم لنقل ترددات منخفضة مثل شبكات التليفون الأرضي .

CAT 2 الفئة الثانية :-

- يستخدم لنقل البيانات الرقمية Data
- ٤ أزواج من الاسلاك
- سرعتها 4 mbps
- تستخدم في توصيل Ring

CAT 3 الفئة الثالثة :-

- السرعة 10 mbps
- ٤ أزواج من الاسلاك
- المسافة 100 m

CAT 4 الفئة الرابعة :-

- السرعة 16 mbps
- المسافة 100 m
- تستخدم في الشبكات ذات التوصيل الحلقي RIng

CAT 5 الفئة الخامسة :-

- السرعة 100 mbps
- المسافة 100 m

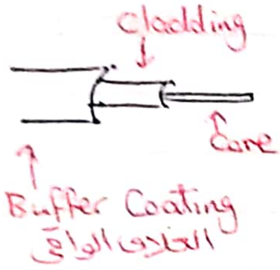
CAT 6 الفئة السادسة :-

- مجدولة بطريقة أكثر من CAT 5
- تحمي من المجال الكهرومغناطيسي سواء رقائق معدنية او سلك مجدول Braided
- السرعة CAT 6 ← 1Gbps
  CAT 6A ← 10 Gbps
- المسافة 100 m

CAT 7 الفئة السابعة :-

- مجدولة بطريقة أكثر من CAT 5
- تحمي من المجال الكهرومغناطيسي سواء كانت رقائق معدنية او سلك مجدول Braided بالاضافة لعزل كهرومغناطيسي خاص لكل زوج منفصل
- السرعة 10 Gbps
- المسافة 100 m

[3] Fiber_optics كابلات الألياف الضوئية



- تعتمد في نقل البيانات على نبضات كهربية
- حيث أن الألياف البصرية الياف مصنوعة من الزجاج النقي وهي طويلة ورفيعة ولا يتعدى سمكها سمك الشعرة وتستخدم للنقل لمسافات بعيدة.

تتكون من

[1] Core القالب النواه

اسطوانة رقيقة جداً من الزجاج رفيعة جداً ينتقل خلالها الضوء

[2] cladding العاكس

يغطي القالب ويعمل على عكس مستمر للضوء داخل الاسطوانة

[3] Buffer Coating الغلاف الواقي

غلاف بلاستيكي يحمي المكونات من الضرر

← الكابل الفايبر للتوصيل يحتاج الى 2 Core للتوصيل بين نقطتين واحد للاستقبال واخر للارسال.

مميزات Fiber

[1] سريعة جداً قد تصل سرعتها من 100 mbps حتى 200 Gbps

[2] مسافة طويلة قد تصل الى 100 Km

[3] مستوى امن عالي حيث انه لا يمر عبر ومضات ضوئية ولا عبر اشارات كهربية

[4] يمكن تحديد الياف بصريه عديده بداخل الكابل مما يسهل التركيب

[5] مضادة للمجال الكهرومغناطيسي EMI

التداخل الكهرومغناطيسي electro Magnetic Interference

[6] لا تتأثر بالماء فيمكن استخدامها في المحيطات

عيوب Fiber

صعوبة التركيب والصيانة لانها تتكون من الزجاج وقد يتكسر عند الانحناء والنواه Core الحديثة مصنوعة من البلاستيك ولكنها لا تستطيع توصيل الضوء لمسافات طويلة كما في حالة الزجاج

← الضوء ينتقل في خط مستقيم ولكن ماذا سيحدث اذا كان المسار منحنى ؟

في هذه الحالة يتم وضع مرآة عند الانحناء حتى يتم عكس الضوء داخل المسار ويستمر هذا الانعكاس حتى يصل الى الطرف الاخر. ويمكن عن طريق هذا الانعكاس يصل الضوء لمسافات طويلة لأن الجدار لا يمتص الضوء

difference between single mode fiber and multi mode fiber.

SMF → Single mode fiber	MMF → Multi mode fiber
→ high Capacity قدرة استيعابية	→ lesser Capacity than SM
→ More Costier than (MM)	→ cheaper than (SM)
→ Light pulses are generated by injection Laser diades [ILDS] نبضات الضوء تولد عن طريق حقن ثنائي الليزر	→ Light pulses are generated by Light emitted diodes [LEDS]
→ Transmission rate of 100 mbps at distance 80/90 Km	→ Transmission rate 100 mbps / 2 Km
→ optimized to allow one light path	→ optimized to allow multi light path

Network devices
اجهزة الشبكات

[1] → NIC = Network interface card   كارت الشبكة

- كارت الشبكة الذى يمكن الجهاز من الاتصال بالشبكة حيث انه يحول ال data الى Binary
- مهمته
[1] الوصول المادى physical
[2] تتعامل مع الطبقة الأولى Network access layer حيث انها تستطيع تحديد المرسل والمستقبل عن طريق Mac address
- أنواعه:
[1] ethernet → يستخدم كابلات الشبكة
[2] wifi → كارت شبكة لاسلكى

← يمكن لكارت الشبكة أن يكون مستقلا ويتم تركيبه فى اللوحة الام herboard لجهاز الحاسوب أو جزء مدمج من اللوحة الام ولا يمكن فصله built in

[2] Repeater :-

→ used to regenerates the signal

← يستخدم لتقويه واعادة توليد الاشارة حيث ان الاشارة تضعف اثناء نقل البيانات لمسافات طويلة بسبب مقاومة السلك او Noise.

← يستخدم في التوصيل الخطي Bus Topology عندما تكون المسافة بين الاجهزه طويلة تحتاج الى تقويه

← يتعامل مع الطبقة الاولى Network access layer.

← هناك نوعين [1] ethernet [2] wireless

← يوجد نوعين حسب تقويه الاشارة

[1] Analoge → يقوم بتكبير الاشارة و ميز بين الاشارة الاصلية والتشويش

[2] Digital → يقوم بتوليد الاشارة لتصبح مثل الأصلية

[3] HuB :- المجمع

→ It is multiport Repeaters عدة بورتات من الريبيتر

← يستخدم في التوصيل النجمي Star topology ويقوم هذا الجهاز بوظيفة الجهاز المركزي

← يستطيع التعامل مع الطبقة الاولى network access layer

حيث انه لا يستطيع ان يميز بين الاجهزه ويرسل لجميع الاجهزة فكلما زادت عدد الاجهزه قلت سرعة الشبكة مما يسبب Loop

↳ send bit out to all ports except the receiving ports.

ترسل البيانات لجميع ماعدا البورت المرسل

- can't understand IPs or Macs

انواعه :-

[1] passive HuB المجمع الخامل :- يقوم باستقبال الاشاره وتمريرها دون تكبيرها فلا يحتاج لتيار كهربي

[2] Active HuB. المجمع النشط :- يقوم باستقبال الاشارة واعادة توليدها ثم يتم تمريرها للتيار الكهربي

4 Switch ⇄

- It is Centeralized device that Can provide physical star topology
← يستخدم فى الاتصال النجمى
- It doesn't know the final Ip but know Macs it is layer 2 device

← يختلف عن HUB فى انه يستطيع تحديد المستقبل عن طريق العنوان الفيزيائى ولكنه لا يفهم IP لانه يستطيع التعامل مع الطبقه الثانيه فقط.

- Mult port of Bridge — عبارة عن عدد بورتات من البريدج
- It operate by hardware ASIC - In LAN

[Application Specific Intergrated Circuit] دوائر متكاملة

يقوم بالعمل عن طريق هاردوير وهو ASIC

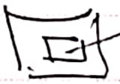
أنواع الـ Switch

	Managed Switch	unmanaged Switch
الخواص والاداء	يستطيع أن يدعم تعديلات للمنافذ ports وعكسه عمل Configuration ويدعم بروتوكلات خاصة بـ Ip Routing Vlan	لا يدعم تعديلات او بروتوكلات خاصه بالتعديل لكنها بروتوكلات خاصة بالتشغيل فقط play and plug
الحماية	قوية	ضعيفه
التكلفة	عالية	ضئيلة
المكان	الشركات الكبيرة	الشركات الصغيرة والمنازل
طبقات نموذج الانترنت التى يتعامل معها	يتعامل مع الطبقة 1، 2، 3 فيستطيع تحديد المكان عن طريق Mac address و Ip address	يستطيع التعامل مع الطبقة الاولى والطبقة الثانيه و network access layer ويفهم Mac address

5 Bridge:- 

← يشبه المكرر Repeater في اعادة الشبكه و يشبه
switch في انه يميز Mac addres لذلك هو يستخدم لتقسيم الشبكة
الكبيرة لشبكات أصغر لتقليل التصادم Colloission domain
ولكنه لا يستطيع نقل بين شبكتين مختلفتين.

← كيف يعمل ؟



→ It is operate by Software
[Cpu + Program in Memory]

• Max of Ports = 16　is only 16 Frame
يستطيع أن يخرج ١٦ حزام فقط

← ماهو Collosion domain ؟

عندما يستقبل الجمع الرزم packets من المنفذ Port يقوم بارسالها
لجميع ports مما يؤدى الى ازدحام الشبكة فادخل استخدام Bridge
لتقسيم الشبكة و لكن استخدامة قبل التفعيل switch

← ماهو الفرق بين Bridge و Switch ؟

الـ Bridge يتعامل مع الداتا كـ Software وبالتالى فهو جهاز بطئ
ولكنه يقسم الشبكة لـ Broadcast domain بينما switch يستخدم
ASIC وهو يتعامل مع الداتا كـ Hardware وبالتالى
يرسل الداتا بسرعه و يقسم الشبكة الى Broad Cast

6 Router :- الموجه



- It is centeralized device that support by s/w different Communication technology.

يستطيع ان يقوم بالربط بين انظمة شبكات مختلفه

- It understand both final Ip and next hop [mac]
- It is layer 3 device

← هو الجزء الاساسي لشبكات الحاسوب وعمودها الفقري وله المقدره على التعامل مع انواع مختلفه من الشبكات و يستطيع ان يفهم Ip address - Mac address

← يقوم بتحويل جميع الحروف الى WAN ويقوم بالتوصيل بينهم عن طريق WAN switch

→ NIC = Network Interface Card
LIC = LAN Interface card
WIC = WAN Interface Card

ماهو الفرق بين Router و Managed switch ؟

أن الروتر Router يستطيع أن يتصل بعده شبكات في وقت واحد بينما Managed Switch لا يستطيع ذلك.

7 Gateway:- بوابه العبور

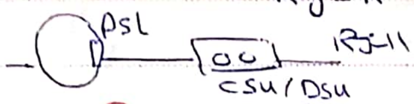
هذا الجهاز او البرنامج يمكن أن يقوم بربط أجهزة الشبكات ويعمل في كل طبقات Internet Model و يستطيع ان يتعامل مع شبكتين كلاهما له بروتوكلات خاصة و يعمل كمترجم بين الشبكات

← يتعامل مع جميع طبقات Tcp / Ip model

8 Digital Modem [modulator (معدل الإشارة) - Demodulator (غير معدل الإشارة)]

→ provide clocking and synchronization

← يستخدم للتحكم في السرعة ويخرج الداتا من RJ-11



→ CSU-DSU = [channelized service unit Data Service unit]

له اسم اخر وهو csu_dsu

9 Server الخادم

جهاز له امكانيات وقدرات عالية وذاكرة فائقة وسعة تخزين عالية وسرعة معالج عالية

أنواع Server حسب الاستخدام:-

1. المخصص one server :- يوفر خدمة واحدة للزبائن وهي مثل printer

2. غير المخصص multi server :- يعمل على توفير عده خدمات للزبائن مثل استرجاع البيانات

9 Firewall الجدار الناري

جهاز أو برنامج يتحكم في الوصول للشبكة حيث ان هذا الجدار الناري لهدف الحماية ويعمل على ضبط الدخول وهذا لعمل security ويكون Hardware او Software

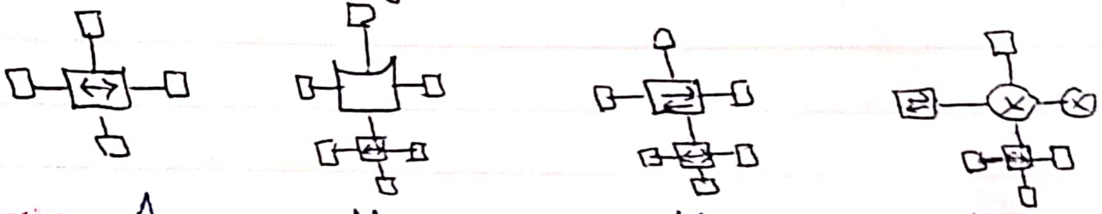
windows firewall → used for secure Internal network.

10 WAP [wireless access point]

يقوم بتوزيع الشبكة المحلية LAN ويتعامل مع L_1 و L_2

(ex)

	HuB	Bridge	Switch	Router



	HuB	Bridge	Switch	Router
Collision domain [unicast] →	1	4	4	4
Broadcast domain →	1	1	1	4
	↑ مش بيميز بيبعت للكل	mac	mac	Ip

[II] exchange server :-

سيرفر يستخدم لارسال واستقبال Message وهو يتعامل مع تطبيقات مثل Microsoft outlook ويستخدم بروتوكولات مثل IMAP - PoP3 - SMTP حتى يتمكن من الوصول للعملاء

exchange server ← بيقوم بالتحكم بكل الايميلات الموجودة في الشركة داخليا ولا يمكن الدخول لها من الخارج الا عن طريق تحويل الدخول بمعرفة Ip الخاص بالسيرفر وهو يتمكن من تحويل الايميلات على السيرفر الرئيسي .

exchange server Requirement :- المتطلبات

← Active directory

عبارة عن Resource لها اكثر من مهمة

[create user - permission user]

حيث ان exchange server لازم يكون على domain ولا يمكن على workgroup

← exchange server member

يعني لازم يكون Join في domain لكي يستطيع ان يقرأ users

[12] Backup Server: سيرفر النسخ الاحتياطي

سيرفر بيقوم بتخزين البيانات احتياطياً حتى يمكن الرجوع لها بحيث يتم تحديد الفايل اللى هيتم عمل له Backup والموعد وممكن أكثر من مرة في اليوم

أنواع Backup :-

[1] Full Backup: الكامل نسخ احتياطي كامل لكل الملفات الموجودة

[2] Incremental Backup: نسخ احتياطي للملفات التي حصل فيها تغيير فقط

[3] Differential Backup

بيقوم بالنسخ الاحتياطي للملفات فقط التي حدث لها تغيير في اخر عملية

التخزين يكون في:

① تخزين محلي: يكون التخزين موصول بجهاز [قرص خارجي مثلاً]

② تخزين خارجي: تلقائي عبر شبكة خارجية

⇒ Backup Requirement:- المتطلبات

يحتوي server Backup على فتحة ethernet خاصة بعملية Backup لأنه هيأثر على النت لانه يقوم بعمل Backup كل شوية وبالتالي هيأثر على النت.

Scanned with CamSca

الموضوع التاريخ: / /

** الأدوات المستخدمة لتنصيب شبكة الحاسوب :

1 Stripping Tool : القشارة

تستخدم كأداة لتعرية كابل الشبكة من العازل البلاستيك ويمكن استبدالها Cutter ولكنها هي الأدق.

2 Crimping Tool : الاراجة

تسمى مكبس الموصلات وهناك نوعين منها

أ) مكبس موصلات :- احدهما يستخدم لكبس موصلات كابل التليفون مع وصلة RJ-11 ذات ٤ أطراف والأخر لكبس كابل الشبكة مع وصلة ذات ٨ أطراف RJ-45

ب) مكبس كابل محوري coaxial cable مع وصلة BNC

3 punch down Tool : دباسة الاسلاك

يستخدم في تدبيس اطراف الاسلاك في كل مكبس RJ-45 أو في لوحات التجميع patch panel ومنها نوعين

← دباسه عادية لتدبيس طرف واحد في المرة .

← دباسه ذات أطراف حادة لقطع السلك الزائد وتدبيس طرف واحد في المرة

4 Network Cable Tester جهاز فحص كابلات الشبكة

جهاز لفحص الكابلات واختبارها قبل الاستخدام

[5] Connectors :- الوصلات

→ Fiber Connectors
- → SC → Square connector
- → ST → Straight tip connector

→ Copper Connectors :-
- → DB = D Shaped  شكل حرف D

[1] DB-60   [2] DB-15   [3] DB-21   [4] DB-9

→ RJ = Rejected Jack

RJ-11	RJ-45
. تتكون من ٤ اسلاك	. تتكون من ٨ اسلاك
. يستخدم للهواتف ADSL-Modem	. يستخدم في ethernet في الكمبيوتر
. يدعم 24 mbps	. يدعم 10 Gbps
. مربع	. مستطيل

طرق توصيل EIA/TIA للكابلات 8 pins ٨ خطوط

→ [1] Straight through Cable : توصيل التقابل المباشر

طريقة للتوصيل بين جهازين مختلفين [PC + روتر] او [روتر + سويتش]

→ used to Connect DTE To DCE

بحيث بيكون في الجهازين نفس ترتيب الاسلاك.

← هناك نوعين من الترتيبات

RJ-45 pinout T-568A

1. white green ابيض اخضر
2. green اخضر
3. white orange
4. blue
5. white blue
6. orange
7. white Brown
8. Brown

(Tx: 1, 2 — Rx: 3, 6)

RJ-45 pinout T-568B

1. white orange
2. orange
3. white green
4. blue
5. white blue
6. green
7. white Brown
8. Brown

← في الغالب يتم استخدام Standard B

← يتم استخدام سلك 1,2 ← Transmission ← Tx ارسال

3,6 ← Receive ← RX ← استقبال

4, 5, 7, 8 → PoE power over ethernet

بيستخدموا لامداد الجهاز بالكهرباء للشحن مثلاً

[2] Cross over Cable: توصيل المعكوس

يستخدم فى حالة توصيل جهازين متماثلين 2DTE و 2DCE مثلاً
يكون الجهاز الاول T-568 B و الاخر T-568 A أو العكس

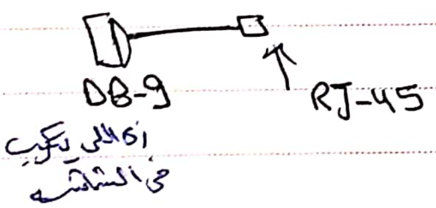
(B)			(A)		
ابيض برتقالى	1	Rx	Tx	1	ابيض اخضر
برتقالى	2	Rx	Tx	2	اخضر
ابيض اخضر	3	Tx	Rx	3	ابيض برتقالى
اخضر	6	Tx	Rx	6	برتقالى

هناك اجهزة تحتوى على auto sense تقوم بالتبديل مباشرة دون تغيير ترتيب الاسلاك

[3] RollOver : التوصيل المقلوب

يستخدم فى حالة توصيل الروتر أو السويتش او الروتر لضبط الاعدادات
used for Console port [Configuration only]
يتم فيه تبديل الكابلات بالعكس

1 → white orange	1 → brown
2 → orange	2 → white brown
3 → white green	3 → green
4 → blue	4 → white blue
5 → white blue	5 → blue
6 → green	6 → white green
7 → white brown	7 → orange
8 → brown	8 → white orange



Connect a computer DB-9 Connector to an RJ-45 cisco Console Cable

Classing Network Components

DTE [data terminal equipment]

- It is adevice that can be source or destination for data and Information
  جهاز قد يكون هو مصدر الداتا او المستقبل
- It understand Ip It is layer 3 or more
- Router → end device

L7
L6
L5
L4
L3 → DTE
L2
L1 → DCE

DCE [data Communication equipment]

- It is adevice that can either provide physical star topology
- provide clocking and synchronization
- It is layer 2 or 1
- wifi HuB - Switch Modem

معدات التجميع وتوزيع الكابلات :

→ [1] patch panels :- لوحات التجميع

switch ← Patch panel ← RJ-45

هي لوحة تجميع حيث أن كل الاجهزة تتصل بها في النهاية وتستخدم التوصيل النجمي Star topology حيث ان كل جهاز يتصل بـ Node سواء اجهزة الحاسوب أو الطابعات وتتصل بكابل Straight يتم توصيله الى مكبس في الحائط RJ-45 وهذا المكبس يتصل بـ patch panel والذي يتصل في النهاية بـ Router أو Switch بكابل Straight through Cable

← Patch Cable ← الكابل الموصل بين patch panel و switch

→ [2] Cabinets :- الكابينة

تستخدم لتثبت اجهزة الشبكة مثل لوحات التجميع والتوزيع Switch و Router ليتم توصيل مع كابلات الشبكة

← منها المثبت في الأرض او في الحائط وتحتوي على مراوح تهوية وأحياناً يكون مبرد عن طريق التكييف وبها أبواب

→ [3] Rack أرفف التوزيع

مثل Cabinets ولكنها لا تحتوي على أبواب أو وسائل للتهوية

الموضوع   التاريخ: / /

POP ←
HTTP ←
SMTP ←

Protocols

→ SSL
→ FTP
→ TCP

البروتوكول protocol = مجموعة rules التي تحكم الاتصال وهي الخطوات المتفق عليها بين مصدر الارسال sender والمستقبل receiver لنقل وتبادل البيانات الرقمية

البروتوكولات تنقسم الى قسمين :-

[1] Connection oriented ← بروتوكولات تقوم باجراء الاتصال المباشر بين اجهزة الشبكة ومن اشهرها TCP

[2] connection less ← هي البروتوكولات لا تسمح بالاتصال المباشر مع PC ويعد بروتوكلات IP

ports - Sockets →

كل بروتوكول يكون له port يعمل عليه وعددها يكون من 0 ← 65535 ولكن هناك بروتوكلات محجوزة لبروتوكلات محفوظة

port n (2^{16}) → 65535 port

[0 - 1023]
→ Well known for service
→ used by server
[HTTP - FTP - —]
بيكون مسجل وخاص بالسيرفرات

[1024 - 65535]
↓
user defined

مسجل registered
[1024 - 49151]

dynamic
[49152 - 65535]

→ un registered ports
→ used by users

This PC → local disk [C]
system32 ← windows
↳ drivers → etc
مسار البروتوكولات في الجهاز

التاريخ: / /　　　　　　　　　　　　　　　　　　　　الموضوع:

فى شبكات Tcp / Ip تنتقل المعلومات من الـ port فى الجهاز المرسل ← المعلومة الى port فى الجهاز المستقبل حسب رقم الـ port

* protocols :-

1. Ip [Internet protocol]

بروتوكول مسئول عن نقل البيانات من نقطة لنقطة ويعتمد على Tcp / Ip ولا يحتوى على اى برمجيات والـ Header الموجود فى Ip هو الذى يحتوى على معرفة الوجهة datagram والتى سيتم توجيهها

2. SNMp [simple network mailing protocol]

[simple network Management protocol]

هو بروتوكول يستخدمه المسئولين لمعرفة معلومات عن الشبكة مثل Routers و Switches لمراقبة الشبكة

3. FTp [file transfer protocol]

هو المسئول عن نقل البيانات فى الشبكة والمسئول عن عملية upload و download

4. Trivial file Transfer protocol [TFTp]

نسخة مصغرة من FTp وتستخدم فى Boot Image للاجهزة التى لا يوجد فيها Boot disk

5. SMTp [simple mail transfer protocol]

هو المسئول عن send الـ emails وتم تطويره الى ESMTp ← extended SMTp

6 pop [post office protocol] Pop3

هو المسئول عن استقبال emails ومعروفة بـ Pop3 وفي بعض الأحيان يقوم باستخدام IMAP مكانه.

7 IMAP [Internet mail access protocol]

بروتوكول يستخدم لاستقبال emails وهو المستخدم في yahoo

← ماهو الفرق بين IMAP و Pop3 ؟

IMAP يمكن فتحه من أي جهاز لأنه يأخذ نسخة على server ولا يتأثر حذف البيانات من على الجهاز كما في Gmail

Pop3 لا يقوم بفتح الايميل من على أكثر من جهاز لأن الداتا تكون مسجله على الجهاز المستخدم فقط ولا توجد نسخة على server فإذا تم حذف البيانات من على الجهاز لا توجد على الايميل

8 Telnet [Terminal Emulation]

الاتصال والتحكم بالشبكه عن بعد عن طريق هذا الـ protocol

9 ICMP [Internet Control Message protocol]

→ Troubleshoot end to end Connectivity

بروتوكول يقع بداخله استخدام بروتوكولين وهما

1. ping → packet Internet groper
2. Tracert → Test Hop to Hop Connectivity to end

وأهميته في معرفة القدرة على التوصيل ويتم فتحه عن طريق [Cmd].

10 HTTP → [hyper text transfer protocol]

هو البروتوكول المستخدم في Internet protocol حيث انه يعمل على نقل البيانات ويعمل على استقبال الصفحات HTML [هدفه التصفح]

11 HTTPS [HTTP secure] encrypted

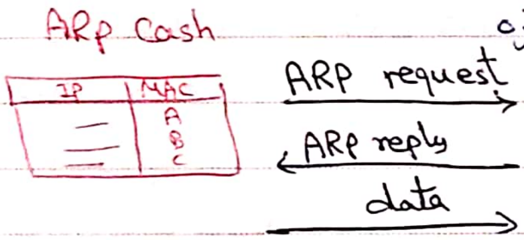
تشفير جميع البيانات بشهادة SSL فلا يتم فك الشفرة الا بين المرسل والمستقبل وهذا لتوفير حماية أكثر.

12 ARP [address resolution protocol]

هو بروتوكول الاتصالات السلكية واللاسلكية المستخدمة لتحليل الشبكة بحيث انه يقوم بتجميع معلومات عن Hardware physical الخاصة بـ IP عن طريق Mac address الموجود في الشبكة ليتم معرفة IP

← مهمته معرفة اقرب جهاز سيتواصل من خلاله

حيث يقوم الجهاز بارسال طلب لجميع الاجهزه Broadcast حتى يتم التعرف على الروتر ويتم ارسال الداتا.



→ The ARP table Contain [dynamic-Static]

13 RARP [Reserve address resolution protocol]

يقوم بعمليه عكس ARP وهو ان يعرف Mac عن طريق IP

14 NTP [Network time Management]

هو بروتوكول يعمل على توحيد الوقت على الاجهزه او عمل Synchronize

وهذا توقيت يعمل على توحيد الساعة العالمية لانه اذا حدث اختلاف في التوقيت تضيع المعلومات

[13] UDP [user datagram protocol]

اداه تعمل في طبقة Transport وهو يستخدم في نقل البيانات مثل الفيديو والصوت بسرعه كبيره وسريع الاداء ولكنه غير موثوق حيث يتم استخدامه في Youtube

[14] DNS [domain name server] او [domain name system]
او [domain name service]

DNS Cash

name	Ip
google	8.888

نظام يتم بداخله تسجيل اسماء المواقع وال Ip الخاص بهم بحيث يمكن الوصول للموقع من خلال اسمه فقط
هناك مؤسستين مسئولين عن Ip

IANA → المسئولة عن البيع
WWW → المسئولة عن التسمية

DNS Request →
DNS Reply ←

← عند الدخول على الجهاز مثلاً ويصل الى البحث ونكتب Facebook فهو يقوم بالاتصال بـ Root DNS لمعرفة الموقع

← يوجد على مستوى العالم 13 Root Hint يعني main DNS server يتم الرجوع لهم.

← أي شركة تحتوي على DNS وتقوم بتسجيله على Server وبتقوم بتحديث هذا الجدول كل ٢٤ ساعة والموقع الذي لم يتم استخدامه لمده ٢٤ ساعه يقوم بحذفه وإذا طلبه أحد يستعلم من Root Hint

DNS → port 53 يعمل على
- TCP → Zone Transfers من سيرفر لسيرفر
- UDP → Query من عميل لسيرفر

15 DHCP [dynamic host Configuration protocol]

← هو البروتوكول المسئول عن اعطاء كل جهاز Ip مستقر عن طريق DHCP Pool ولكي يقوم DHCP بهذه العملية لازم يكون authorized في Active directory

→ DHCP authorization registers the DHCP Server Service in the active directory domain to support DHCP clients

← الجهاز الموجود الذي لا يحتوي على Ip يقوم بـ 4 خطوات لكي يصل الى Ip من DHCP server

الجهاز → السيرفر

- DHCP discovery [Broadcast] →
- ← DHCP offer
- DHCP accept, Request Reservation →
- ← DHCP Acknowledgment

ماهو DHCP offer ؟ هو عرض من DHCP server يحتوي على 4 مكونات

Ip address	
Mask	
default gateway	
DNS	

17 SSL [secure socket layer]

بروتوكول طبقة المنافذ وهو يعمل على مستوى عالي من الامان

18 LDAP [Light weight directory access protocol]

ترجمة البروتوكول الخفيف ويستخدم لتعديل الأدلة

19 PPTp [Point to point tunneling protocol]
PPP [Point to point Protocol]

هو بروتوكول يستخدم لجعل جهاز بعيد الاتصال بالشبكة وهو موجود في data layer

Port Number	Application	
80	HTTp	TCp
443	HTTps	
21	FTp	
25	SMTp	
23	Telnet	
53	DNS	UDP
67	DHCP	
161	SNMP	
69	TFTp	

→ Dynamic ARp Table entries:-

are created wherever the windows Tcp/Ip stack makes an ARp request and the Mac address isn't found in the ARp table the ARp request is Broadcast on the local segment when the Mac address of the request Ip address is found, that Information is added to the ARp table.

MAC [media access Control]   Next Hop

→ Is aphysical address burnt on Rom of NIC [hardware]
عنوان يتم طبعه على الجهاز

→ 48 bit address
→ used to send data Hop to Hop
→ It is represented In hexadecimal
النظام السادس عشر

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
A → 10, B → 11, C → 12, D → 13, E → 14, F → 15

تتكون من ١٢ حرف

٦ رموز: __ __ __ | ٦ رموز: __ __ __

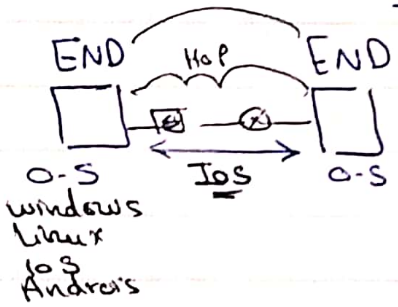
OUI   Host part

↳ [organisation unique Identifient]

جزء خاص بالشركة لا يتغير وجزء خاص بالعميل هو المختلف

Network Model

Network model: It is agroup of Concepts (مبادئ) that will help adevice to send data hop by hop and then end to end



كل جهاز عليه نظام تشغيل O.S [operating system]

وللاتصال بين الشبكات لابد من network model

[1] DoD model [department of defense model]

← يطلق عليه TCP/IP (transfer Control protocol / Internet protocol)

← تم اعداده من قبل DARPA

← تم اعداده لدعم وزارة الدفاع الامريكية بحيث تم وضع بعض المعايير والقيود للتطوير ومن هذه المعايير

① لا يخضع لشركة معينة او تطبيق معين

② يحتوي على ادوات صيانة بداخله للقيام بالصيانة في حالة وجود مشكلة

③ امكانية الاتصال بين الشبكات

← يصف الاتصال في ٤ layer وليس ٧ كما في OSI

← TCP هو الجزء المسئول عن نقل البيانات والربط ويقسم هذا البروتوكول الجزء من البيانات الى اجزاء صغيرة للتعامل معها وتسمى هذه الاجزاء datagram والذي يحتوي على معلومات وتحتوي على العنوان المستقبل والمرسل وتسمى Header وتحتوي على Checksum وهي معادلة للفحص ووصول البيانات للنقطة المرسلة.

2 OSI Model [open system Interconnection]

→ open Standard and open Source model

موديل قابل للتعديل وهو referencey model يستخدم للدراسة فقط لمعرفة مراحل انتقال البيانات حيث انه يتكون من 7 layer وبينما المستخدم في الواقع هو Tcp/Ip model

→ approved by ISo [International standard organisation]

→ Make Standarization to main task for operation by IEEE.

IEEE → معهد Institute of electrical and electronic engineers

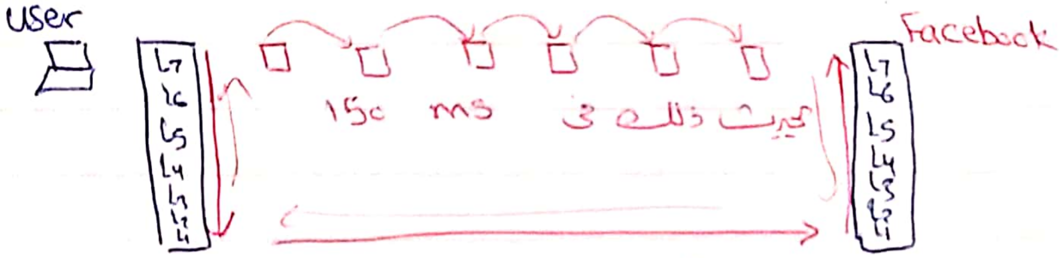
→ Network model consist of layers that layer is functions that can be done by S/W or H/W that functions are مترتبة sequentional.

OSI model		Tcp/Ip model
L7 : application layer	→ HTTP - FTP - SMTP	L4 : Application layer
L6 : presentation layer	← data →	
L5 : Session layer		
L4 : Transport layer	[header | data part] segment	L3 : Transport layer (TCP, UDP)
L3 : Network layer	header [Src IP, dst IP | segment] packet	L2 : Internet layer (IPv4, IPv6)
L2 : Data link	Header [| packet | CRC] Tail; Src mac, dst mac	L1 : Network Access layer
L1 : physical	Frame	

1 Application Layer: L7

It is responsible for proper data preparation for proper service

هذه الطبقة المسئولة عن التطبيقات مثل Google chrome وهذه التطبيقات
تستخدم البروتوكلات مثل HTTP_FTP_SMTP_Telnet_POP3
البث المباشر RTP → (real time transfer protocol)



عند الرغبة في الوصول الى facebook يمر الاتصال من ال L7 الى L1

2 presentation Layer: L6

→ It is responsible for finding Common data between sender & receiver

مسئولة عن قراءة البيانات وتحديد نوعها extension

ex: ASCII → text Avi, mpeg → video JPG, Gif → picture

← هي طبقة العرض المسئولة عن تهيئة البيانات والتفريق بين كل نوع من البيانات حيث عند نزول البيانات من طبقة Application الى طبقة presentation تقوم هذه الطبقة بعمل تصنيف.

← في هذه الطبقة يتم عمل ضغط للبيانات Compression من قبل المرسل و فك الضغط decompression من قبل المستلم

وكذلك التشفير Encryption و Non-encryption عدم التشفير

3 Session layer: L5

→ It is responsible for make sure that all data which required for open session is ready and then give orders.

→ Session Establishment انشاء

→ Session Management & Control

→ Session Termination انهاء

Subject _ to بتقوم بمراجعة كل الامر المرسل مثلا الايميل
لو فيه مشكلة تقوم بابلاغ العميل

← هي طبقة المسئولة عن عمل جلسة وادارة و فتح واغلاق الاتصال
حيث انها المسئولة عن الدخول على Facebook .
وتستطيع تحديد نوع الاتصال [Simplex_half duplex_Full duplex]

4 Transport layer: L4

→ It is responsible for actual (التنفيذ الفعلي) Mechanics for

1. Session establishment
2. Session Management & Control
3. Session Termination

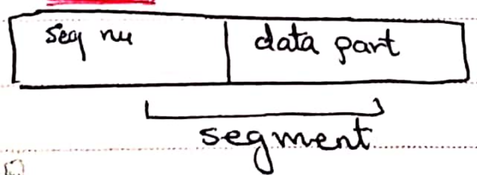
← حيث انها الطبقة المسئولة عن نقل وادارة البيانات وتحديد نوع البيانات المرسلة والمستقبلة وتقوم بتحديد نوع البروتوكول المستخدم

TCP → Transmission Control Protocol محافظة البيانات

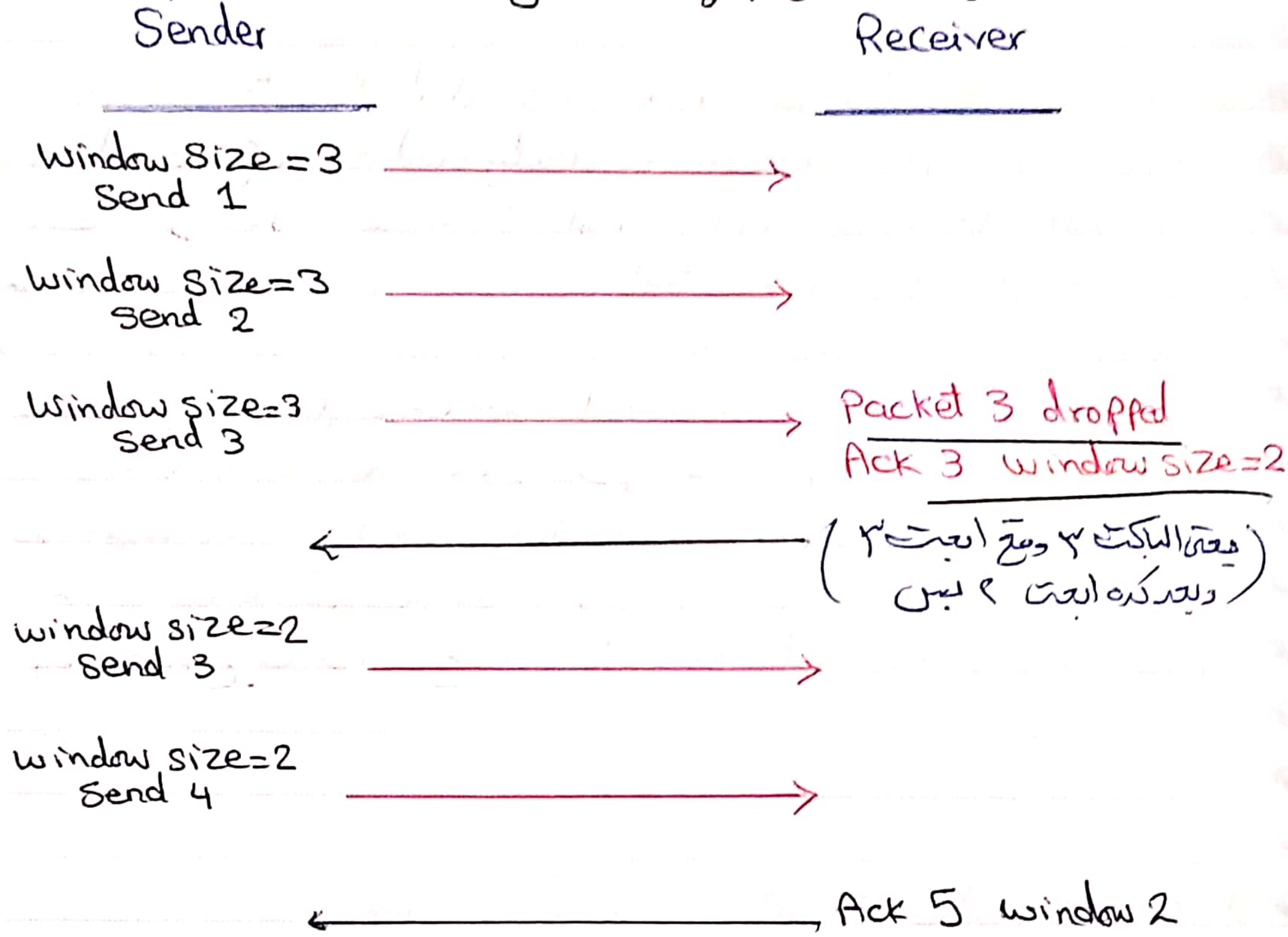
UDP → User datagram protocol

← في هذه الطبقة يتم تقسيم الداتا الى Segments اجزاء

Header



← هذه الطريقة تعمل بطريقة Windowing في TCP فقط



وهكذا ويتم التأكيد على كل جزء قبل ارسال التالي حتى يتم الانتهاء

وهذا يحدث في TCP فقط بينما في UDP يتم التأكد مرة واحدة بأن هناك مستقبل وبعد ذلك يتم ارسال الـ Data دون تأكد

الفرق بين TCP و UDP

TCP	UDP
• Transmission Control protocol	• User datagram protocol
• Connection oriented [reliable]	• Connection less [un reliable]
تتأكد من ارسال البيانات بالكامل بحيث انه اذا لم يتم الارسال بالكامل يقوم باعادة ارسالها مرة اخرى	لا تتأكد من ان الداتا قد تم ارسالها ام لا بحيث انه قد يرسل الصورة وبها تقطيع
• slower but reliable	• fast but Non guaranated transfer (best effort)
• Typical Application [Email _ web Browsing] FTP-HTTP-SMTP-DNS-PoP3	• Typical application - VoIP DHCP - RTP - DNS (user - server)
• unicast	• unicast - Broadcast - Multicast
• Tcp sequence format 20 byte	• UDP sequence format 8 byte

8 byte:

Source port 2	destination port 2
length 2	2 CRC

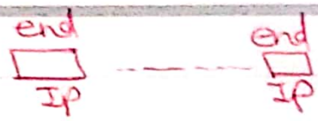
• يتم في هذه الطريقة ٣ أشياء

① Segmentation (تقطيع) : divide data to small parts called segments.

② CRC [cyclic Redundancy check] تصحيح الداتا بحيث لو فيه مشكلة حصلت في ارسالها

③ Addressing by port number [65535] ترقيم الداتا عن طريق رقم البورت

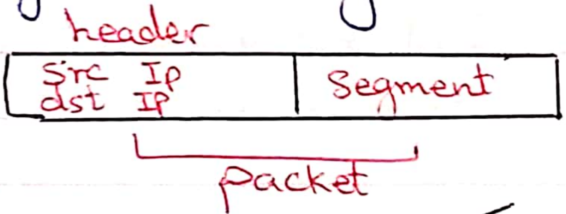
5 Network Layer :- L3



→ responsible for end to end delivery data by using Ip
توصيل البيانات من النهاية الى النهاية

يتم في هذه الطبقة تحويل الـ segment الى packet حيث يتم اضافة الـ header الـ Src Ip , dst Ip وبهذه الطريقة يتم توجيه packet الى المستقبل وهذه العملية تسمى routing وهي تتم باستخدام بروتوكولات مثل [ospf-RIP-EIGRP]

→ logical addressing → choose the best path from src to dst.



وفي هذه الطبقة يتم استخدام بروتوكولين هما

1. Ip → Internet protocol
2. ICMP → Internet Control Message protocol

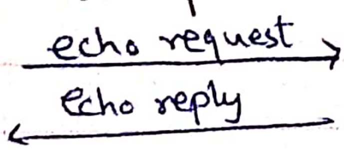
↩ هو بروتوكول يستخدم لمعرفة مدى قدرة الاتصال ويتم استخدام اداتين لذلك

1. Ping ← cmd → ping Ip

وهو المستخدم لمعرفة مدى القدرة على التوصيل حتى النهاية

ping command

1. To test abasic Ip connectivity
2. uses the ICMP Sending Called an ICMP echo request to another Ip address
3. The Computer with Ip should reply with an ICMP echo reply



يعني يبعت رسالة للجهاز الي عليه الـ Ip المطلوب
لو قام يرد عليه بـ echo .

ع لو فيه مشكلة بيبعت رسالة مثل

Error Message ك [Request time out = destination unreachable]

① Request time out → معناه ان الجهاز المطلوب غير موجود.

② destination unreachable → معناه ان فيه جهاز اخر بيرد ويبلغ ان الجهاز مش موجود

طرق القيام بهذا ال Command

(ex)

→ Ping 192.168.2.2 هيبعت 32 bit packet ويرد عليك ٤ مرات

→ Ping 192.168.2.2 -l 1500

هيبعت packet مساحة حتى 1500 bit حتى يتأكد من مدى التوصيل

→ ping 192.168.2.2 -n 10 هيقوم بالارسال حتى ١٠ مرات

→ ping 192.168.2.2 -t

هيستمر في الارسال حتى توقفه بـ ctrl+C

cmd → Tracert www.yahoo.com   Tracert [2]

Trace on Router _ Tracert on PC

تتبع مسار بحيث يوضح كل Hops اللي بيمر عليها حتى الوصول.

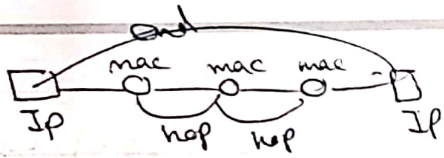
- To trace the hops between 2 points on network
- This Command show your every router Interface a Tcp/Ip packet passes through its way to a destination

- every router decrease TTL [time to live] by 1

يعني ان كل روتر هيعدي عليه هيقلل TTL بمعدل 1

Scanned with CamScanner

6 Data Link layer : L2



→ responsible for end to end delivery data by mac address

← وهي الطبقة التي يتم فيها تجهيز البيانات لتوصيلها للشبكة وتقوم بتغليف packet وتحويلها الى Frame

header

src mac dst mac		CRC 4 byte

↑ Frame ↑

← قد تسمى LLC ← Logical Link Control حيث ان هذه الطبقة طبقة التحكم المنطقية بحيث يتم وضع في هذه المرحلة Mac address الخاص بالجهاز وهو لا يتكرر

← يتم في هذه الطبقة عمل فحص CRC

CRC → depend on mathematical equation

وهي معادلة تقوم بتصوير الداتا قبل الارسال وعند الوصول وعمل مقارنة بينهم وهذا حتى يتم معرفة اذا كان هناك مشكلة يقوم باعادة ارسالها مره اخرى وكذلك حتى ١٦ مرة فاذا لم يتم الارسال كامل يتم الابلاغ بالفشل

⇒ Mac Frame :   لماذا حجم الباكت ١٥٠٠ بايت فقط ؟

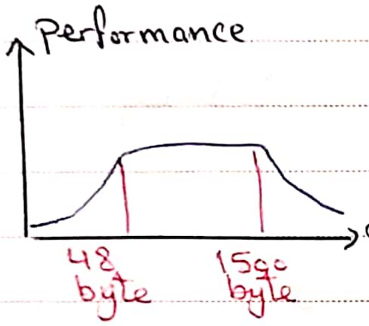
8 byte	6 byte	6 byte	2 byte	1500 byte	4 byte
pre	dst mac	src mac	type	packet	CRC

pre → pre data

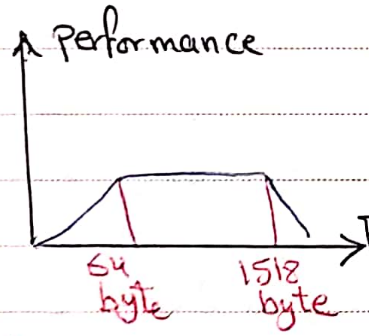
عبارة عن كهرباء في البداية للتنشيط وهي تقوم بالتحكم في سرعتها وضبطها

Auto clocking & synchronization

Src mac → Source mac   المرسل
dst mac → destination mac   المستقبل
type → type of packet   نوع الباكت IPv4 ام IPv6
CRC → FCS [frame check sequence]   الفحص



MTU = Maximum Transfer unit = 1500
max Packet size = 1500 byte
اقل نقل لـ packet هو 48 byte واكثر هو 1500 byte
min Packet size = 48 byte



Min frame size = 18 + 64 = 64 byte
Max frame size = 18 + 1500 = 1500 byte

ليه حجم الا packet 1500 byte خلاله Frame 1518 وليس 1526 خاطا
هناك predata مساحتها 8 byte ؟
يتم الغاء predata من اول packet والـ packet التالي يحتوي على 8 byte عبارة عن Idle time الموجود بين باكتين فيكون حجم الـ Frame الثابت

6 byte [Src mac] + 6 byte [dst mac] + 2 byte (type) + 4 byte (CRC) + 1500 byte (packet) = 1518 byte

7 physical Layer :- L1

→ Convert data to Signals
- defines network media type
- defines Cables types
- The physical component must be supported by data-link Layer.

→ Convert frame to Bits [01001 0 ...]

---

packetizing :- عملية التغليف

← لكي يتم ارسال البيانات من Sender الى Receiver ينبغي تقسيم
data الى اجزاء تسمى Frame ثم اضافة بعض المعلومات
في header ويكون فيها عنوان المرسل والمستقبل
وفي النهاية يتم اضافة Trailer

Header	data	Trailer
المقدمة		النهاية

Tcp Header

Source port		Destination port	
Sequence Number			
Acknowledgement Number			
offset	Reserved	Flags	window
check sum		urgent pointer	
options		padding	
start of data			

-> Source port: يعبر عن المكان الذى يرسل البيانات

-> Destination port: يعبر عن المكان المرسل له البيانات

-> Sequence Number: رقم المسلسل الخاص بال datagram لتسهيل عملية اعادة تنظيم البيانات على الكمبيوتر

-> Aknowledgement Number: رقم يتم من خلاله المرسل معرفة ان تم الارسال

-> offset: يعبر عن طول ال header ككل

-> Reserved: متغير يتم الاستفادة منه فى أى شئ اخر اضافى

-> Flags: تعبر عن معلومات مهمة جداً

-> window: تعطى امكانية زيادة حجم ال packet مما يؤدى الى دقة نقل البيانات

-> urgent Pointer: يعطى تصريحاً بأهمية البيانات

-> options: مجموعة متغيرات يمكن الاستفادة منها فيما بعد

-> padding: يستخدم للتأكد من ان ال header توقف عند 32 bit

-> Start of data: بداية المعلومات الحقيقية التى سيتم نقلها

Routing ← التوجيه يقوم بفحص العنوان الموجود على الرزمة packet ويعطيه تصريح تجول فى ارجاء الشبكة وهذا التصريح له مدة محددة TTL ← time to live فاذا انتهت هذه المدة فقدت الرزمة.

Ip Header

Version	IHL	Tos	Total length
Identification	Flags		Fragmentation offset
Time to live	protocol		header checksum
Tcp header			
Start of data			

- Version : تعبر عن رقم اصدار Ip [IPv4 - IPv6]
- IHL [Internet header length] طول الـ header وقد يكون من 5 كلمات مضاعفات 32 bit
- Tos [type of service] تعبر عن أهمية البيانات المطلوبة
  ← وهي عبارة عن اعطاء الأولوية حسب الرقم وهما من 0 → 7
  → reflect the priorities the highest is the best الأولوية الأعلى
  - data → 0, 1, 2, 3 download - upload - email
  - video → 4
  - voice → 5
  - Router protocol → 6
  - Switch protocol → 7

  (↓ الأفضلية)
- Total Length : تحدد طول الداتاجرام ولها قيمة 65535 byte
- Identification : تعريف يجعل الجهاز المستقبل يستطيع اعادة ترتيب datagram
- Flags : اول bit في datagram يعبر عن انها غير مقسمة بينما اخر bit يعبر عن انها مقسمة
- Fragmentation offset : يعبر عن المكان المحدد للمعلومات
- Time to live [TTL] : (remove layer 3 Loop)
  الوقت المحدد لنقل packet بعد ان ينتهي هذا الوقت تصبح مفقودة والـ Hop
  دائماً ما يكون 32 Hop

Numbering System

*data unit of measure

Bit = 0,1   Byte = 8 Bit   KB = 1024 Byte

MB = 1024 KB   GB = 1024 MB   TB = 1024 GB

(MB ↑ Mega)   (GB ↑ Giga)   (TB ↑ Tera)

المحتويات	الأساسي	اسم النظام
0,1	2	Binary System النظام الثنائي
0 → 9	10	Decimal System النظام العشري
0 → 7	8	octa system النظام الثماني
0 → 9, 10 → A, 11 → B, 12 → C, 13 → D, 14 → E, 15 → F	16	hexadecimal النظام السادس عشر

Bit Bosition	7	6	5	4	3	2	1	0
Binary exponential	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Value of Bit	128	64	32	16	8	4	2	1

IpV4

* IPV4 ⇒ Internet protocol version 4

- it is used for communication
- an Ip serves two main functions host or network Interface Identification and location addressing.
- It is responsible for
  1. Logical addressing (Ip v4 addressing)
  2. Encupsulation data end to end

- Types of IpV4:-
  1. A private Ip address:-
     is an Ip address that reserved for Internal use behind a router or other network address Translation (NAT) device apart from the public.

  2. A public Ip address:-
     it is public and can't be used within a home or a business work.

** يعني أن هناك نوعين من Ip نوع داخلي وهو private وهو يستخدم داخل LAN ونوع خارجي يوصل بالإنترنت وهو public وللتحويل بين الاثنين نحتاج الى شئ وهو خدمة NAT
Network address Translation

* IP V4 Formation :-

→ An IPv4 address is a 32-bit address that is typically written in dotted-decimal notation, such as 192.168.1.1.

→ no of Ip = 2^{32} = 4,000,000,000

• IPv4 represented in dotted decimal :-

يعني ← انه بيتكون من 4 octet كل octet بيتكون من 8 bit كل Bit له قيمة حسب مكانه

7	6	5	4	3	2	1	0
X	X	X	X	X	X	X	X
128	64	32	16	8	4	2	1

octet / 8 bit . ____ . ____ . ____

* بنحوض مكان 1 بقيمتها بينما bit 0 قيمته 0

• ex: 10101010 , 11111111 . 00000000 . 00001111
170 , 255 . 0 . 15

←

* IPv4 classes:

[I] Class A :- [Network . Host . Host . Host]

mask 255.0.0.0 /8

← الاوكتيت الاول فقط خاص بالشركه وثابت بينما ٣ الاخرين متغيرين

يتم استخدامها في الشركات الكبيرة .

- no of Ip = 2^{24} = 16.777.216

ex:- 41.X.X.X

Network ID = 41.0.0.0

First ID = 41.0.0.1

Last ID = 41.255.255.254

Broadcast ID = 41.255.255.255

اول رقم واخر رقم محجوزين

* Network address :

This is the designation used in routing to send packets to a remote network for example.

10.0.0.0 172.16.0.0 192.168.10.0

* BroadCast address:

The address used by applications and hosts to send information to all nodes on a network is called the broadcast address

1 حتى → 126 بتكون من

2) **class B :** [Network . Network . Host . Host]

mask 255.255.0.0 /16

← اول أوكتتين محجوزين للشركة، والاثنين الاخرين متغيرين

* Start from [128 ⟶ 191] اول أوكتيت

no of Ip = $2^{16} - 2 = 6634$ Ip

3) **class C :** [Network . Network . Network . Host]

mask 255.255.255.0 /24

← أول ٢ octet ثابتين و ال octet الاخير متغير

* Start from [192 ⟶ 223]

no of Ip = $2^{8} - 2 = 254$ Ip

* class A, B, C ⟶ unicast Ip

4) **class D :-** * Start from [224 ⟶ 239]

← يستخدم multi cast

← يستخدم في الالعاب online كل جهاز يكون له Ip خاص به و Ip خاص باللعبه

5) **class E :-** * start from [240 ⟶ 254]

يستخدم في

① Researches الابحاث

② Military Application التطبيقات العسكرية

* Ip must give each LAN its own Identifier
Network IDs:-
- All Computers on same LAN must have same Network ID.
  كل الشبكات في نفس LAN لازم تحتوي على نفس ID عشان نعرف هي بعض
- Each Computer on same LAN must have a unique Host ID.
  كل جهاز على الشبكة LAN يجب ان يكون له ID منفرد

* CIDR : classless Inter domain Routing
* IPs are reserved:- IPs محجوزة

[1] 0.0.0.0
→ All IPV4 network address خاص بشبكة الانترنت كلها

[2] 127.0.0.1 → Reserved for Loopback
→ It is used for Ip Test

[3] 255.255.255.255
→ General and public broadcast for all IPV4 devices
→ local Broadcast (Non routable) inside LAN only.

التاريخ: / /   الموضوع

+ Ipv4 shortage:-

فى سنة 2000 وجدوا انهم يتبقى غير 5 % فقط من Ip لأن كل عميل كان يشترى class كامل.

Network المطلوب	class	wasted Ip غير المستخدم
6 Ip	class C → 256 Ip	250 Ip
536 Ip	Class B → 65535 Ip	6500 Ip
377,216 Ip	class A → 16,777,216	16,400,000 Ip

→ Ipv4 Solutions:-

① New version:-

① IPV5
(64 bit) used for researches only

② Ipv6
(128 bit) 2^{128} = ---- Ip
معدل → 5×10^{28} Ip/Human

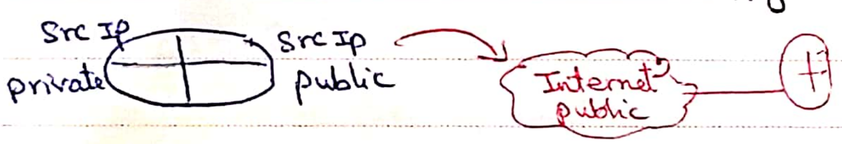
② private IP
مجانية

③ Subnetting
شبكات فرعية يعنى تقسيم الشبكة الى اجزاء

SENA

Public Ip	Private Ip
• Required by devices and Hosts that connect directly on the Internet ← بيقوم باستخدامه من المستخدمين العاديين • must be globally unique ← يجب ان يكون منفرد • Routable on the Internet يستطيع ان يخرج على الانترنت • Must be assigned by IANA / RIR IANA → Internet Assigned Number Authority مؤسسة مسؤولة عن الارقام	• Not Routable on the Internet لا يخرج على Internet → class A 10.0.0.0 /8 → class B 172.16.0.0 → 172.31.0.0 /12 → class C 192.168.0.0 /16 • Can be assigned Locally by an organisation • must be translated to access the Internet

← كل Ip في public له سعر 1 $/year



← الروتر المنزلي يحتوي على Private Ip ولكنه عند خروجه على الانترنت يأخذ Public Ip وهذا عن طريق S/W وهو NAT

NAT → network address translation

** APIPA (Automatic private Ip address)

عند عدم حصول ال Host على Ip ولم يحصل على Ip من DHCP يأخذ Ip Non routable وهنا Ip يمكن استخدامه في Workgroup فقط

وهذا ال Ip من IANA

169.254.x.x /16

① APIPA only usable by Microsoft operating systems
② All addresses will fall in the range
169.254.0.1 ⟶ 169.254.255.255
③ Most Microsoft operating systems failover to APIPA if no othe addressing is available.
④ Many routers and switches Intended for home users use APIPA as a default settings.

IPv4 Subnetting — الشبكات الفرعية

* Subnetting :- divide Major network to subnets
تقسيم الشبكة الكبيرة إلى شبكة فرعية

→ An IPv4 Configuration Identifies a computer to other Computers or networks.

→ CIDR :- classless Inter domain Routing

Class C

ex 1) 192.168.0.0 /24 — كم شبكة وكم Host

الحل

/24 = 255.255.255.0

∴ التغيير في آخر octet تبعاً لـ class C

0 → [00000000] آخر اوكتيت

عدد الشبكات = $2^{\text{أس}}$ [أس = عدد الوحايد الموجودة في الاوكتيت المتغير] — Network

عدد المشتركين = $2^{\text{أس}} - 2$ [أس = عدد الاصفار في آخر اوكتيت] — Network, Broadcast

no of Host = $2^8 - 2 = 256 - 2 = 254$

no of Network = $2^0 = 1$

Network ID → 192.168.0.0
First Host → 192.168.0.1
Last Host → 192.168.0.254
Broadcast ID → 192.168.0.255

Subnetting → take apart of host bits and assign it to network part

→ origin Ip

| N | H |

→ Subnetting Ip

| N | SN | H |

- Subnet mask:-

① 32 bits mask that differentiate between host bits and network bits
② Continuous of 1'S

EX2 192.168.0.0 /25

الحل

/25 → 11111111.11111111.11111111.10000000 → 255.255.255.128

no of Hosts = $2^7 - 2$ = 128 − 2 = 126

no of Network = 2^1 = 2

* التغيير في اخر octet

يتم تقسيم الشبكة الى شبكتين

	Network 1	Network 2
Network ID	192.168.0.0	192.168.0.128
First Host	192.168.0.1	192.168.0.129
Last Host	192.168.0.126	192.168.0.254
Broadcast	192.168.0.127	192.168.0.255

ex 3　192-168-5-0 /24　　5 subnet , 30 Host

الحل

← هو عايز الشبكة تتقسم على الأقل الى 5 Subnet

no of Network $= 2^n \geq 5$　　n=3　　∴ أخر اوكتيت هيكون فيه ٣ واحد

11100000

255-255-255-224 ⟶ /27

no of Host $= 2^5 - 2 = 30$ Host　　تبعاً لأخر اوكتيت

no of Network $= 2^3 = 8$

كده هتقسم الى ٨ شبكات بهم ٣٠ Host

	Network 1	Network 2	Network 3	Network 4
Network ID	192.168.5.0	192-168-5-32	192.168.5.64	192-168.5.96
first Host	192.168-5-1	192-168-5-33	192.168.5.65	192.168.5.97
Last Host	192.168-5-30	192-168-5.62	192.168.5.94	192.168-5.126
Broadcast	192.168-5.31	192.168.5-63	192.168.5.95	192.168-5.127

	Network 5	Network 6	Network 7	Network 8
Network ID	192-168-5-128	192-168-5-160	192-168-5.192	192-168-5.224
First Host	192-168.5.129	192-168-5-161	192.168.5.193	192.168-5-225
Last Host	192.168-5-158	192.168-5-190	192.168.5.222	192.168.5-254
Broadcast	192-168-5-159	192-168-5-191	192-168-5-223	192.168.5.255

ex4   192-168-5.0 /24   5 12 Subnet

المطلوب

No of Network = $2^n \geq 12$ $n=4$

1111

new mask /28 → 255.255.255.240

no of network = $2^4 = 16$ Sno of Host = $2^4 - 2 = 16 - 2 = 14$

	Network 1	Network 2	Network 3	Network 4
Network ID	192.168.5.0	192.168.5.16	192.168.5.32	192.168.5.48
first Host	192.168.5.1	192.168.5.17	192.168.5.33	192.168.5.49
Last Host	192.168.5.14	192.168.5.30	192.168.5.46	192.168.5.62
Broadcast	192.168.5.15	192.168.5.31	192.168.5.47	192.168.5.63
	Network 5	Network 6	Network 7	Network 8
Network ID	192.168.5.64	192.168.5.80	192.168-0.96	192.168.5.112
first Host	192.168.5.65	192.168.5.81	192.168.5.97	192.168.5.113
Last Host	192.168.5.78	192.168.5.94	192.168.5.110	192.168.5.126
Broadcast	192.168.5.79	192.168.5.95	192.168.5.111	192.168.5.127
	Network 9	Network 10	Network 11	Network 12
Network ID	192.168.5.128	192.168.5.144	192.168.5.160	192.168.5.176
first ID	192.168.5.129	192.168.5.145	192.168.5.161	192.168.5.177
last ID	192.168.5.142	192.168.5.158	192.168.5.174	192-1685.190
Broadcast	192.168.5.143	192.168.5.159	192.168.5.175	192.168.5.191
	Network 13	Network 14	Network 15	Network 16
Network ID	192.168.5.192	192.168.5.208	192.168.5.224	192.168.5.240
first Host	192.168.5.193	192.168.5.209	192.168.5.225	192.168.5.241
Last Host	192.168.5.206	192.168.5.222	192.168.5.238	192.168.5.254
Broadcast	192.168.5.207	192.168.5.223	192.168.5.239	192.168.5.255

Class B

EX1 172.16.0.0 /17

الحل

17 → 255.255.$\overset{1}{128}$.0

- التغيير في اخر ٢ أوكتيت لانه class B

no of Network $= 2^1 = 2$

no of Host $= 2^{15} - 2 = 32,768 - 2 = 32,766$

هتقسم الى شبكتين مع ملاحظة أن التغيير سيكون في اخر اوكتيتين وكل اوكتيت الحد الاقصى له 255

	Network 1	Network 2
Network ID	172.16.0.0	172.16.128.0
First Host	172.16.0.1	172.16.128.1
Last Host	172.16.127.254	172.16.255.254
BroadCast	172.16.127.255	172.16.255.255

Ex2 170-1-0-0 /16 → 5 subnet

الحل

no Network $= 2^n \geq 5$ $n = 3$ 111ooooo

new mask → /19 → 255.255.224.0

no of network $= 2^3 = 8$

no of Hosts $= 2^5 - 2 = 32 - 2 = 30$ Host

← مع ملاحظة ان التغيير سيكون في اخر ٢ اوكتيت لان ذلك class B

	Network 1	Network 2	Network 3	Network 4
Network ID	170-1.0-0	170-1.32.0	170.1.64.0	170-1.96.0
First Host	170-1.0.1	170.1.32.1	170.1.64.1	170.1.96.1
Last Host	170.1.31.254	170.1.63.254	170.1.95.254	170.1.127.254
Broadcast	170.1.31.255	170-1-63-255	170.1.95.255	170.1.127.255

	Network 5	Network 6	Network 7	Network 8
Network ID	170-1-128.0	170-1-160.0	170.1.192.0	170-1-224.0
First Host	170-1-128.1	170-1-160.1	170.1.192.1	170-1.224.1
Last Host	170-1.159.254	170-1.191-254	170.1.223.254	170-1.255.254
Broadcast	170-1.159-255	170-1.191.255	170.1.223.255	170-1.255.255

Class A

ex1 10.0.0.0 /8

الحـــــل

/8 → 255.0.0.0

no of network = $2^0 = 1$ ، no of host = 2^{24} = 16.777.240

شبكة واحدة

Network ID → 10.0.0.0   First Host → 10.0.0.1

BroadCast → 10.255.255.255   Last Host → 10.255.255.254

ex2 10.0.0.0 /9

الحل

/9 → 255.128.0.0 (10000000)

no of network = $2^1 = 2$ ، No of Hosts = 2^{23} = 8.388.608

← مع الملاحظة أن التغيير في آخر ٣ اوكتيت لانه class A

	Network 1	Network 2
Network ID	10.0.0.0	10.128.0.0
First Host	10.0.0.1	10.128.0.1
Last Host	10.127.255.254	10.255.255.254
Broadcast	10.127.255.255	10.255.255.255

جدول العلاقة بين Subnet mask و Hosts

bit location	7	6	5	4	3	2	1	0
class A	9	10	11	12	13	14	15	16
class B	17	18	19	20	21	22	23	24
class C	25	26	27	28	29	30	31	32
bit value	128	64	32	16	8	4	2	1
value	128	192	224	240	248	252	254	255

يتم استخدام هذا الجدول عن طريق عدد Hosts نعرف mask

Cisco exam

[1] 192.168.1.50 /27

الحل

class C   32 Host ⟵ 27 ← Subnet mask تبع الـ

Network ID → 192.168.1.32
First Host → 192.168.1.33
Last Host → 192.168.1.62
Broadcast → 192.168.1.63

2 192.168.1.20 /29

الحل

/29 → 8 host — class C → التغيير في رابع اوكتيت

Network ID → 192.168.1.16 — Broadcast → 192.168.1.23

First Host → 192.168.1.17 — Last Host → 192.168.1.22

3 170.1.20.3 /21

الحل

/21 → 8 host — class B → التغيير في ثالث اوكتيت

Network ID → 170.1.16.0 — Broadcast → 170.1.23.255

First Host → 170.1.16.1 — Last Host → 170.1.23.254

4 10.50.2.3 /11

الحل

/11 → 32 host — class A التغيير اول ٢ اوكتيت

Network ID → 10.32.0.0 — Broadcast → 10.63.255.255

First Host → 10.32.0.1 — Last Host → 10.63.255.254

5 10.20.1.2/13

الحل

/13 → 8 host — class A

Network ID → 10.16.0.0 — Broadcast → 10.23.255.255

First Host → 10.16.0.1 — Last Host → 10.23.255.254

6 CIDR :- is short for Classless Inter domain Routing which three of the following Ip addresses belong to the CIDR block of 115.64.4.0/22 ? [Choose three]

A - 115.64.12.128

B - 115.64.7.64

C - 115.64.6.255

D - 115.64.5.128

الحل

الاختيارات هتكون B,C,D لان subnet mask /22 يحتوي على 4 Host وتبعا

ل classA ع ـا في المسألة التجريبية من تاني octet و ٣ شبكات يفضلوا

في تاني Subnet بينما A في التالتة .

7 The subnet mask is 255.255.252.224 which three addresses below Could you assign to network hosts ? [choose three]

A - 217.63.12.192

B - 92.11.178.93

C - 134.17.18.56

D - 192.168.16.87

الحل

الاختيارات B,C,D ل السؤال ايه IPs اللي ينفع اديها Hosts

فاكيد مش هيكون Network ID , ول Broadcast

VLSM

VLSM :- Variable length Subnet mask

- variable length Subnet mask were developed to allow multiple Levels of Subnetted Ip addresses within a single network
تقسيم Subnet الواحد الى عدة VLSM حتى يمكن الاستفادة من جميع Ips

- The Routing protocol you use must support VLSM
  [RIP2] Routing information protocol version 2
  [EIGRP] enhanced Intergatway Routing Protocol
  [OSPF] open Shortest path first

- VLSM is crucial (حاسم) for an effective (مؤثر) Ip addressing

example

192.168.1.0 /24 ⇒ A = 60 Host , B = 30 Host
C = 14 Host , D = 6 Host , E = 6 Host

الحل

← اكبر عدد من Hosts مطلوب هو 60 وتبعاً ل class C
فإن Subnet mask سيكون /26

no of Network = $2^2 = 4$, no of Hosts = $2^6 - 2 = 64 - 2 = 62$

↳ [1] 192.168.1.0   [2] 192.168.1.64
[3] 192.168.1.128   [4] 192.168.1.192

هنقسم كل Subnet على حسب حاجة المستخدم

Subnet A :- 60 Host

192.168.1.64 /26   mask → 255.255.255.192

Network ID → 192.168.1.64   Broadcast → 192.168.1.127
First Host → 192.168.1.65   Last Host → 192.168.1.126

Subnet B :- 30 Host

192.168.1.128 /27   mask → 255.255.255.224

Network ID → 192.168.1.128   Broadcast → 192.168.1.159
First Host → 192.168.1.129   last Host → 192.168.1.158

Subnet C :- 14 Host

192.168.1.160 /28   mask → 255.255.255.240

Network ID → 192.168.1.160   Broadcast → 192.168.1.175
First Host → 192.168.1.161   Last Host → 192.168.1.174

Subnet D :- 6 Host

192.168.1.176 /29   mask → 255.255.255.248

Network ID → 192.168.1.176   Broadcast → 192.168.1.183
First Host → 192.168.1.177   last Host → 192.168.1.182

Subnet E :- 6 Host

192.168.1.0 /29   mask → 255.255.255.248

Network ID → 192.168.1.0   Broadcast → 192.168.1.7
First Host → 192.168.1.1   Last Host → 192.168.1.6

Summarization :- التجميع

→ It is grouping many subnets and advertisment them as a bigger subnet.

→ Routing protocols can summarize addresses of several networks into one address range.

- تجميع عدد Subnets حتى يمكن تمثيلهم ك Subnet واحد

EX.1

172.16.12.0 /24
172.16.13.0 /24
172.16.14.0 /24
172.16.15.0 /24

→ 172.16.12.0/22

الكيفية

- في هذه الحالة class B يعني التغيير في اوكتيت رقم ٣
- نأخذ الاوكتيت الثالث لأول واخر شبكة ونحولهم الى bits

12 ⟶ 00001100
15 ⟶ 00001111

000011   6 bit

- نجمع الاثنين منطقي 1+1=1 ، 0+0=0 ، 0+1=0
ونحسب عدد bit من اخر قيمة وهي 1 وفي هذه المسالة ⟵ 6 bit
- عدد ال bits هو 8+8+6=22   Subnet mask /22:-
- نأخذ اول شبكة ويكون لها subnet mask

172.16.12.0/22

Ex:

192.168.1.0/25
192.168.1.128/26
192.168.1.192/27
192.168.1.224/28
→ 192.168.1.0/24

الحل

← فاهذه المسألة class C يحقا التغيير في اخر octet

00000000
11100000
____
00000000 → 0 bits

mask → 8+8+8+0 = 24

∴ 192.168.1.0/24

Ip V6

IPV6 : Internet protocol version 6

* why we need IpV6?

because we need Larger address space

Ipv4 → 2^{32} = 4,294,467,295 Ip   4 octet = 32 bit Decimal

IpV6 → 2^{128} = 3.4×10^{38} Ip   8 octet = 128 bit hexadecimal

every octet = 4 hexadecimal Digit

→ 1 hexadecimal Digit = 1 Nibble = 4 bits

every octet = 4 x 4 = 16 bit   بتكون من 8 اوكتيت

8 octet x 16 bit = 128 bit

octet = field

Example

2001 : 0db8 : 34cd : 0012 : 0000 : 0000 : 00a9 : 1234

Network Prefix [network address]   Interface Identifier [host address]

* Rules:-

Rule 1:- Left zero can be excluded when we write address:- (اختصار)

الصفر على الشمال يمكن ازالته

2001:0db8:34cd:0012:0000:0000:00a9:1234

↳ 2001:db8:34cd:12:0:0:a9:1234

Rule 2:- Full zero octets can be [::] only one double colon and used only once.

① 2001:0000:0000:0000:0000:0000:0000:000F

↳ 2001::F

② 203B:0000:0000:0000:1234:0000:0000:ABCD

↳ 203B::1234::ABCD (✗)

الاستخدام يكون مره واحده فقط حتى يمكن معرفته هو مستخدم مكان كام اوكتت

↳ 203B::1234:0:0:ABCD (✓)

Ipv4 address	Ipv6 address
→ public (Real)	→ Global
→ APIPA (virtual)	→ link-local
→ private (virtual)	→ site-local
→ loopback [127.0.0.1]	→ Loopback [::1]
→ unspecified [0.0.0.0]	→ unspecified [::]
→ class D Multicast [224.0.0.0]	→ FF00::/8 Multicast من FF01 → FF0F اذا احتوى على FF

⇒ Global Network prefix :-

→ 001   + 45 bit   + 16 bit

يبدأ 001 وهي قد تكون 0011 أو 0010

وهذا يعني ان ISP يستطيع ان يوزع Ip حتى 2^{80} Ip

⇒ Link Local Network prefix :-

→ 1111111010 + 54 bit
→ always begin with FE80
→ Assign automatically for interfaces, routers can't routing these address
→ when host interface assigned this kind of ip addresses it must know its not used by other hosts.

يستخدم طريقة تسمى ب SLAAC أو eui-64 address

SLAAC = State less address Auto Configuration
eui = extended unique Interface

في هذه الطريقة تستخدم Mac address وهو يساوي 48 bit ونضيف عليه FFFE حتى تكمل 64 bit الباقيين

(ex) AAAAAA AAAAAA → AAAAAA FFFE AAAAAA

⇒ Site local Network Interface:

→ Always begin with FEC0 ↗ zero
→ No Auto Configuration with it and assign manually or by DHCP V6.

⇒ IpV4 mapped address:

تحويل V4 الى V6

→ For an IPV4 mapped address, the Last 32 bit of a standard IPV6 address may be written in decimal.

تحويل Ip V4 الى V6 نضع امامه decimal

← 80 bit →	← 32 bit →	← 32 bit →	
0	FFFF	192.168.30.1	IPV4 address

ipv4 mapped address = 0.0.0.0.0.0 FFFF.192.168.30.1

لكن بيل جيتس رفض فقدموا Hybrid Ipv4 Compatible

⇒ Hybrid Ipv4 Compatible:

For the sake of readability the same Ipv4 address can also be noted which decimal numbers as a hybrid Ipv4 Compatible address in which case the address become.

← هنقوم بتحويل decimal الى hexadecimal

::192.0.2.52

96 bits ←→ 0 (0:0:0:0:0:0)   32 bits ←→ Ipv4 address 192.168.0.1

Ipv4 Compatible address = 0:0:0:0:0:0 192.168.30.1
= ::192.168.30.1
= ::C0AB:1E01

طرق تعامل Ipv4 مع Ipv6

[1] dual stack

وضع Ipv4 و Ipv6 على نفس Interface

[2] Tunneling   نفق

① manual Ipv6 over Ipv4 tunneling

← يعمل نفق خيالي من الداخل V4 ومن الخارج V6

← أي وضع Ip v6 packet (encapsulated) داخل Ipv4

ولكن router interface يجب أن يكون dual stack

② dynamic 6 to 4 tunneling

وهي طريقة للوصول الى جزء Ipv6 على الانترنت من خلال Ipv4

حيث يتم اعطاؤه unique prefix الى كل جزيرة في جزء Ipv6

③ Intra site automatic Tunnel addressing protocol

dual stack host Ipv4 Ipv6

④ Tunneling

[3] Nat-pt → Network address Translation

بروتوكول يقوم بتحويل الـ Ipv4 لـ Ipv6 اذا تطلب الامر

Router bootup عند فتح الروتر

Router Internal Components : مكونات الروتر الداخلية

1. power Supply
2. cpu → processor
3. RAM DiMMS →
   RAM
   - → VRAM [Volatile RAM] لازم الرام يفضل متصل بالكهرباء للحفاظ على المعلومات
   - → NVRAM [Non volatile RAM] لا يحتاج الى كهرباء مثل الفلاشة
4. Flash → contain [Ios] Internetwork open System يحتوي على نظام التشغيل
5. Boot RoM
6. WIC → ethernet او serial ports سواء ports يتم تركيب فيها
7. Rom
   - post — Rx BooT
   - Boot strap — RoMMon
   } Initial ios الحصول على o.s المؤقت

Router external Components : مكونات الروتر الخارجية

1. Serial ports → Multi serial
   هو ال port الذي يحتوي على serial والمستخدم للخروج الى WAN
2. Fast ethernet port
   سرعته 100 mbps
3. Console port
4. Auxiliary port } for Configuration
5. power switch
6. power card connection

كيف تتم معرفة Serial ؟

← يتم معرفة port ethernet اذا كان built in بيكون مكتوب عليها ethernet 0/0 ، ethernet 0/1 بينما اذا كان built out بيكون مكتوب على WIC الوكايه اللى داخل فيها W0 مثلاً S0 / S1

⇒ Router bootup sequence :- تسلسل فتح الروتر

---

[1] BIos will Run post to check hardware

BIos [basic input output system]

شبابيه لها password لا تقبل التعديل عند فتح الجهاز يقوم الـ BIos بتشغيل POST ليقوم بعمل فحص لجميع مكونات الجهاز

POST [Power on self test]

[2] BIos will Run BooT to Load operating system

الـ BIos بيفتح BooT لعرفه O.S لتشغيل الجهاز

NVRAM → Contain start file   # show start

VRAM → Contain Run file   # show Run

الروتر بيسجل كل حاجة فى Run فعشان نعمل save للبيانات

↳ # Copy run start

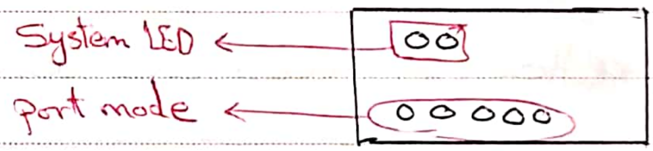
يعني يقوم بنسخ Run من VRAM الى start فى NVRAM

الى يحفظ Configuration file

الموضوع   التاريخ: / /

** port LEDs during Switch POST :-   الفحص عند الفحص

→ At the start, all port LEDs are green → each leds turns off (مغلقة)
→ After its tests completes
  → If a test fails, its LEDs turns amber
→ System LED turns amber if any test fails.
→ If no test fails, post completes, on POST Completion LEDs blink then turn off.



** BooTstrap = Load Ios and Configuration file.

1. Find ios
2. Load ios at the RAM
3. Find Configuration file
4. Load Configuration file at the RAM

Flask → TFTp Server → RoM

أول خطوه وهي ان الروتر عشان يحمل operating system بيروح الى NVRAM
ويحمله من Flash لو مش موجود بيحمله من TFTp
لو مش موجود بيحمله من RoM.

* Cisco IOS installed inside the Router to manage the H/W it is working on.

IOS معمول عشان يدير على الهاردوير

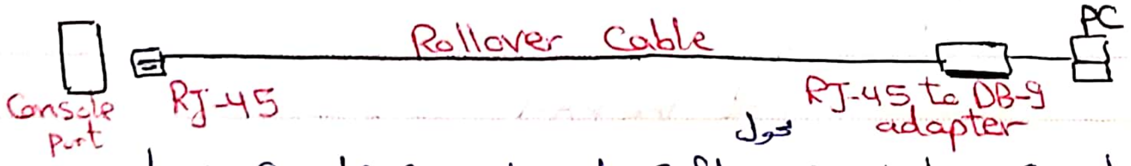
* Configuration file, is a program file that contain information for the Router to tell it how to react & Respond

Configuration file عبارة عن ملف برمجي به المعلومات التي تجعل الروتر يتفاعل .

** How can access Cisco devices　　　　　　　　طريقة التحكم

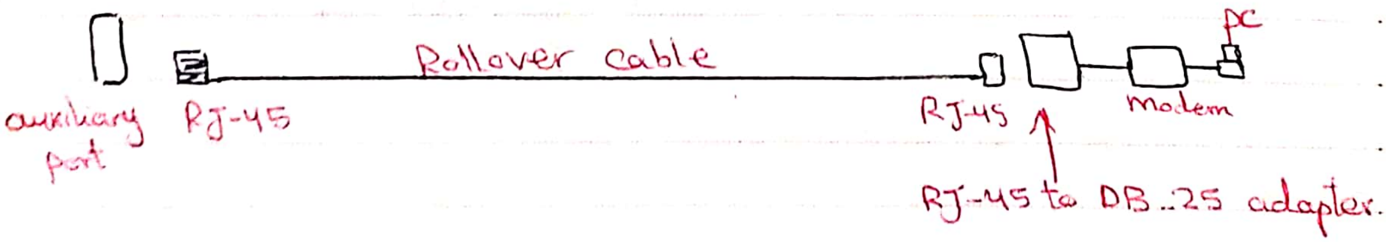
Console port ⎤ ⊗ ⎫ Telnet [virtual]　　　　عن طريق التحكم في device
auxiliary port ⎦ ⊖ ⎭　　　　　　　　　　　　　عن طريق احد ال Port

1 Management port console port connector :



Line Console 0 اسمه Software تحول عليه Console Card ←

2 Management port auxiliary port connector



عمل تسطيب على برنامج cisco ب packet tracer → Configuration on

1) نقوم بتوصيل Router ب Laptop عن طريق Console Cable ودة بيكون عن طريق اختيار Terminal.

2) عند الدخول من laptop على Terminal هيفتح على setup mode وهي صفحة خاصة بإعدادات الروتر هيظهر فيها

→ Continue with Configuration dialogue ? [yes/No]

وفي السؤال ده بيسأل اذا كان يعمل Configuration معد مسبقًا

هنكتب No ثم enter هيظهر Router>

3) عشان ندخل على privilleged mode او enable mode هنكتب enable

ثم enter وهنا هنتحول الى Router #

وهذه المرحلة مسئولة عن بعض الاوامر

privilleged mode → [show - Copy - erase - debug]

للعودة من enable الى setup mode نكتب disable

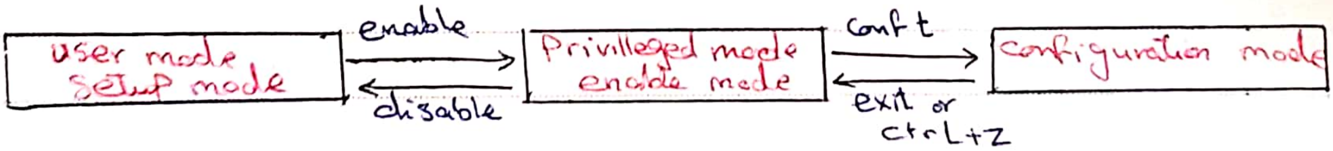
4) للدخول الى المرحلة الثالثة Configuration mode نكتب

Conf t = Configuration Terminal

وهنا هنتحول الى Router (config) #

وفي هذه المرحلة يتم وضع Configuration Command سواء كان اسم الجهاز أو password

← للخروج من هذه المرحلة exit او Ctrl + Z



Configuration Modes

[1] Setup Mode [Initial Configuration mode]

- It is yes/No Configuration dialogue, by default first using [yes/No] Question dialogue
- It used for Quick and Simple Configuration
- To exit from setup mode press [ctrl+c] or [No]

[2] User Mode:- Router > ____ (Router name)

- It is used for Simple Monitering troubleshooting
- Comman prompt :- Router >

[3] privilleged mode [enable mode] Router > → Router

- Include all commands in user mode plus extra advanced Monitering Commands trouble shootings.
- To return to user mode type disable

4 Configuration mode [Global mode]

- To define generic configuration on the router which affect the device [password_name of router]
  → Router # Configure Terminal or Config T
    → Router (config) #
- To exit from configuration mode:- [ctrl+Z or exit] or end

5 Sub_Configuration modes

- Line sub-Configuration mode → Router (config-line) #
- Interface sub_Configuration mode → Router (config-if) #
- Router sub_Configuration mode → Router (config-router) #

Commands In enable mode

→ Router # Copy run start — لحفظ كل الاوامر لـ Start

→ Router # reload — لعمل restart للجهاز

→ Router # show ip route — لاظهار الـ route عليه مثلاً

→ Router # Show run — لاظهار الاعدادات
Show history — التاريخ
Show clock — الساعة

Commands in Configuration mode

→ Router(Config)# host name ____ الاسم

لتسمية الروتر باسم معين

→ Router(Config)# Line Console 0
Router(Config-line)# password ____
Login

لعمل password عند الدخول للجهاز عند فتح الجهاز مباشر

→ Router(Config)# enable password ____

لعمل password لمرحلة enable mode وتظهر في #show run

→ Router(Config)# enable secret ____

لعمل password مشفر لـ enable mode لا يظهر في #show run

→ Router(Config)# no enable password

no قبل كل شيء للغيه مثلاً الغاء باسورد enable

→ Router(Config)# do show run

do قبل اى شئ تفعله في Config T بدلاً من enable

→ Router(Config)# do wr = Router# copy run start

يحفظ كل commands

→ Router (config)# Service password_encryption
#show run في console حتى passwords يقوم بتشفير جميع

→ Router (config)# no Ip domain_lookup
حماية الروتر من عمل loop اثناء عمل Config

→ Router (config)# interface g0/0
Router (config-Int)# no shut down
لجعل Interface دائماً شغالة ولاتفصل

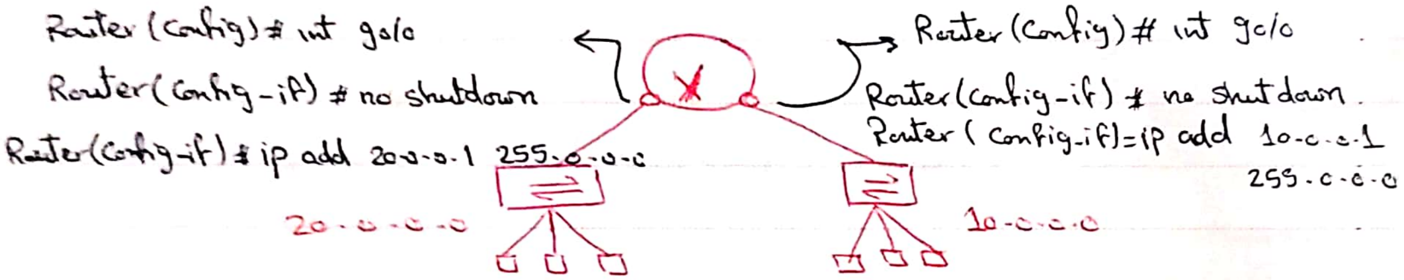
→ Router (config)# interface g0/0
Router (config-int)# no shut down
Router (config-int)# Ip address 20.0.0.100 (Ip) 255.0.0.0 (mask)
لجعل Interface لها Ip

→ Router (config)# clock set 10:56:02 7 Dec 2021
للقيام بضبط الساعة

→ Router (config-if)# Line vty 0 4　　VTy → virtual Terminal
Router (config-line)# password 123　　[port لل security لعمل]
Login
لعمل password على البورتات من 0→4 حتى يمنع اى احد من الدخول
اليه فى remote login بدون الباسورد
Command → Telnet Ip of router
حتى هيدخل الا بالباسورد

الموضوع   التاريخ: / /

كيفيه الدخول على الروتر Remote عن طريق packet tracer



① بعد اعطاء كل Interface الـ Ip تبعاً للشبكة المتصل بها نقوم باعطاء كل PC الـ Ip الخاص به مع مراعاه عند كل جهاز نكتب gateway Ip الخاص به في الروتر وهو 10.0.0.1 او 20.0.0.1 تبع شبكته

② لكي نتأكد من أن الشبكات ترى بعضها نقوم بارسال ✉ من جهاز لاخر او ندخل للـ Command في الجهاز ونكتب
Ping ip of device

وهيظهر ٤ رسائل نعرف منهم اذا كان متصل اولا

③ يمكن الدخول للروتر من الجهاز عن طريق Telnet Ip of router

** Password Recovery :- اعادة تهيئة الباسورد

هنلاقي Router هيجيب IOS ولكن لا يحمل Config file وهيقوم الروتر بالدخول الى Setup mode.

- Set the Configuration Register to by pass the Configuration in NVRAM. (0X2142)

1. To access RoMMon, press (ctrl+break) during booting.
   نعمل restart للجهاز وانناء الفتح نضغط (ctrl+break) هيظهر التالي

2. RoMMoN 1 > Confreg 0X2142 هنكتب الى بالاسود
   RoMMoN 2 > reset

3. we will enter setup mode → ctrl + C → enable
4. Router # Copy start run لكي يحضر النسخة المسجلة run لعمل التعديل
5. change password
6. Router(config)# Config-register 0X2102
7. Router # copy run start لحفظ التعديل

(ملحوظة) بعد تغيير password هنلاحظ ان Router هيفصل عن Switch فلازم ندخل على Interface المتصل ب Switch ونعمل # no shutdown

* Backing up and Restoring of Ios & Configuration files:-

للقيام بعمل نسخ من مكان لمكان نستخدم

Router # Copy Source destination

Source المكان اللى هنسخ منه ، destination المكان اللى هنسخ ليه

← القيام بعمل نسخه للـ Ios احتياطى من Flash الى TFTp (Trivial FTP)

Backup Ios → Router # Copy Flash TFTp

Restore Ios → Router # Copy TFTp Flash

delete Ios from flash → Router # delete Flash Filename

← للقيام بعمل نسخه للـ Configuration file من start لـ TFTp

Back up Configuration file → Router # Copy start TFTP

Restore Configuration file → Router # Copy TFTp start

محو ← Erase Configuration file → Router # erase startup-Confreg

الطريقة الاولى لعمل نسخة احتياطية #show run —Copy→ Text

1. نقوم بعمل # show run ونأخذ copy في Text خارجى
2. نقوم بـ Router #erase startup-confreg هيقوم بمسح كل Configuration
3. للاعادة نقوم بأخذ copy من text ونضعه في paste

Router (Config) # ______

#do wr

4. تم اعادة كل Configuration مره أخرى

** الطريقة الثانية لعمل نسخة احتياطية :-

1) هنضيف Server للشبكة وندية Ip مثلاً 10.0.0.7
عند الدخول على server في packet tracer هنلاقي service فيها Backup موجود فيها عدد Backup وأسمائها

2) بالنسبة للروتر نعمل show version# لمعرفة الإصدار الخاص بالروتر ويكون داخلاً موديل C1900 ، ونقوم بعمل show flash#
عشان نعرف نوع Flash الموجود

3) للقيام بعمل نسخة من TFTP لـ Flash

Router #Copy TFTP Flash
#adress or name of remote host ? 10.0.0.7 → Ip of TFTP server
file name ? ______ نكتب اسم Ios اللي مكتوب في TFTP بالضبط

4) لو عايز Router يستخدم Ios جديد :-

Router (Config)# boot system Flash ______ Ios name ______ اسم الفلاش

في حالة أن الـ Flash ليس بيه مساحة كافية

Router(Config) # boot system TFTP ______ Ios name ______ TFTP Ip address

كده هياخد نسخة مباشرة من TFTP بدلاً من الذهاب إلى Flash

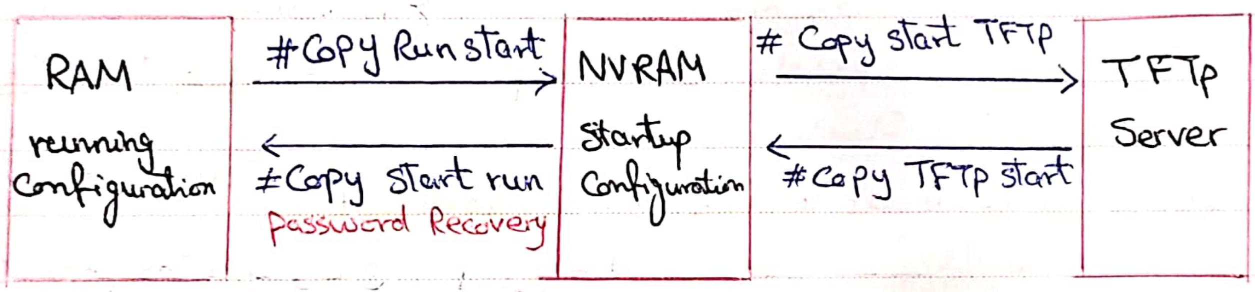
5) لعمل نسخة من الـ Flash اللي شغال إلى TFTP

Router #: Copy run TFTP
- address or name of remote host ? 10.0.0.7 » Ip of TFTP server
File name ? osama
dowr

Notes:-

① If the Configuration register value is 0X2100 it will boot from RoMMON

② If the Configuration register value is 0X2102 it will check the Configuration file in NVRAM for boot system Command if Not found it will Load from first file found in the Flash



CDP = cisco discovery protocoL   بروتوكول لإعطاء معلومات عن الجيران

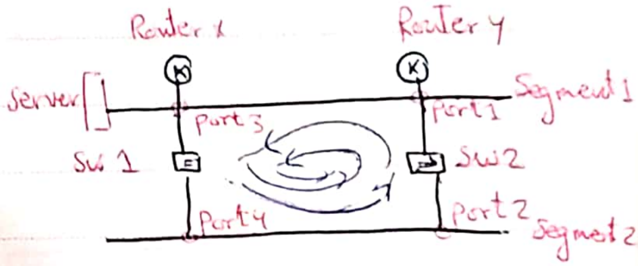
- enabled by default on all cisco devices
- it is Layer 2 protocoL
- cdp discovers basic Information about neighbors cisco device

Show cdp neighbors
Show cdp neighbors detail
Show cdp Interface

[STp]

Spanning Tree protocol

* Redundant Topology الاحتياطي

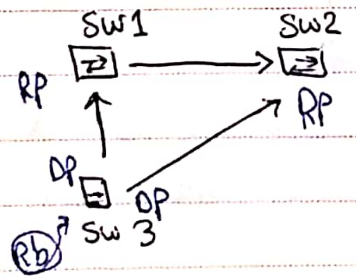


- Redundant topology eliminates single points of failure, Redundant topology causes broadcast storms, multiple frame copies, and Mac address table Instability problems.

عند توصيل سلك احتياطي لحالة سقوط الشبكة يقوم السويتش بعمل Broadcast فتلف الداتا وترجع تاني مما يسبب loop .

- Host X [server] sends a unicast frame to router Y. Mac address of router Y has not been learned by switch yet, Router Y will receive 2 copies of the same frame.
- Switches A and B learn the Mac address of host X on port 0. the frame to router Y is flooded, switches A and B incorrectly learn the Mac address of host X on port 1.

← عشان نمنع loop بنستخدم بروتوكول STP



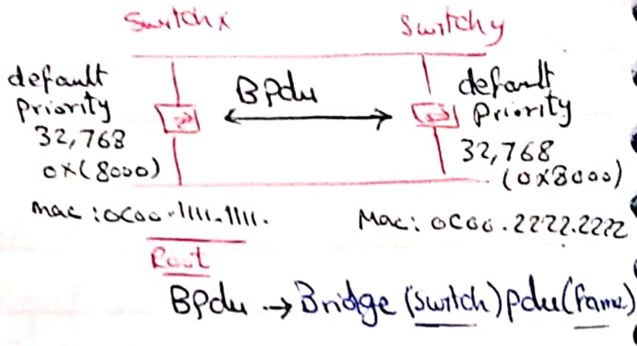
1. one root bridge per network [RB]
2. one root port per non root bridge [RP]
3. one designated port per segment [DP]
4. Non designated port are unused = Alternate port [ALT]

يتم اختيار كبير للسويتشات [Rb] وكل سويتش اخر يتم توصيله به عن طريق [Rp] وهو بيتواصل معاه عن طريق بورت وهو [Dp] وهناك بورتات لا يتم استخدامها [Alt] ، كل بورت هيكون لها Role ← [Root port - designated port]

و State ← Forward

* STP Root Bridge selection :-

→ BPdu default send every 2 seconds
الـ Frame بيتم ارساله في ثانيتين بحد اقصى ٢٠ ثانية .



→ Root bridge is switch having least Switch ID

→ Bridge ID = | bridge Priority | MAC Address |

priority → 16 bit → 32.768 default   ثابت لا يتغير
Mac address → Least Mac address   اقل Mac address

* Root port selection :-

→ It is the best port on-non root bridge that Can reach to Root bridge
→ depend on the lowest cost to root bridge if it equal depend on the lowest port no.

بيعتمد على Cost الاقل بين السويتش والـ Root ولو متساويين بيقا Root no

Cost based on Bw [Bandwidth]
الـ Cost بيعتمد على سرعة التوصيل السرعه الاكثر لها اقل Cost

BW	Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

* designated port Selection:-

→ It is the best port on each Link that can reach to the root bridge.
→ The lowest Cost to root bridge, if equal is the lowest port ID.
هو البورت الاقرب لـ root bridge.

* Blocked [Alternate] port selection:-

→ It is the port that are neigther :- RP or DP

→ Spanning - Tree port states:-

1 disabled :-

- No Cable is Connected
- port is shutdown

2 Blocked:-

- doesn't transmit or receive data frames
- listen to receive BPDUs.
- doesn't transmit BPDUs.

3 Listenting:-

- doesn't transmit or receive data frames
- process BPDUs for root RP - DP election
- first forward delay time = 15 sec

4) Learning :-

- doesn't transmit data frames
- drops the received data frames but after learning the source mac
- process BPUS for Root, RP, DP election
- second forward delay time = 15 sec

5) Forwarding

- Start forwarding data frames
- process BPUS.

* Spanning Tree timer [BPDU Timers]

Hello time → The hello time is the time between each BPdu frame that is sent on a port this is equal to 2 sec, but can be between 1 → 10 sec   زمن ارسال الباكت.

Forward delay → The forward delay is the time spent in the listening and learning state
- This is equal 15 sec for each state but can turned on to be between 4 → 30 sec   زمن قراءة البيانات

Maximum age → The Max age timers Controls the Maximum length of time a switch port saves Configuration BPdu Information
This is 20 sec by default, but can be turned to be between 6 → 40 sec

* Topology Change Notification :- AT change :-

→ If the root bridge goes down :- عند سقوط الـ Root

Link Come up → Blocking [moves to Listening after it decides it is root port a designated port → [1] Blocking [loss Bpdu detected] max age = 20 sec
[2] listening forward delay = 15 sec
[3] Learning forward delay = 15 sec
[4] Forwarding

• Convergence will take 50 sec [20 + 15 + 15]
→ all other switches go to blocking state for → 20 sec then go to listening state for 15 sec then to learning state for 15 sec then the forwarding state.
لتقليل هذه المدة يتم استخدام RSTP

→ RSTP [Rapid STP]

Line Come up → Blocking → [1] Blocking forward delay = 6 sec
[2] listening forward delay = 15 sec
[3] Forward

min Convergence time is 21 sec

يقلل المدة من ٥٠ ثانية الى ٢١ ثانية

** port fast : البورت السريع

— Port fast : It is the port that Jumpes to forward state Immediately

⟵ It is port that connected to pc

عبارة عن جعل الـ port يقفز الى Forward دون المرور الى listen او learn

عند غلق وفتح الاجهزه فلاحظ انها تقرأ بسرعة

lap

→ Router #conf t
Router(config)# int fo/8
Router(config-if)# Spanning-tree port fast
do wr

- لو مطلوب مثلاً يعمل port بسرعه مع اول ٢٤ بورت نستخدم Range

→ Router>en
Router #conf t
Router(config)# int Range fo/1 24
Router(config-if)# spanning-tree port fast
do wr

كيف يقوم ال Switch بتوجيه data ؟

[1] Learning

It is forming mac table by checking Source mac in InComing frames

تكوين جدول بالماكات عن طريق فحص الداتا

mac	table
—	—
—	—
—	—
—	—

→ Switch will Flush Inactive entries after 5 min Inactivity by default.

يزيل اى خادم عند توقف نشاطه ٥ دقائق

→ Switch Can Learn many devices on Same ports but will not learn Same mac on two different ports.

[2] Forwarding:

→ forwarding frames by checking dst mac in frames [Unknown – Broadcast – Multicast]

→ All devices on switch are in the same broadcast domain.

كل الاجهزه على السويتش يتم التعامل معها كدومين

→ forwarding is done by use Micro segmentation

يتم توجيه الداتا عن طريق وحدات صغيره

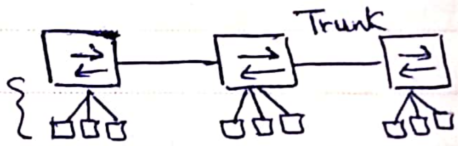
** VLAN

VLAN → Virtual LAN (Local area Network)

. divide main LAN into Sub LANs called VLAN

عبارة عن تقسيم بورتات السويتش الى vlans بحيث أن كل port يكون تابع لـ vlan معينه .

access



← اتصال الـ Switches مع بعضها بيكون عن طريق Trunk mode بينما اتصال الـ Switch مع PC بيكون access mode

** VLAN Importance

1. Reduce overhead (التكلفة) by Limiting the size of each broadcast domain
2. Groups users by department function مقسم
3. enforce better security by keeping sensitive (حساسة) device on aseparate (منفصل) VLAN.
4. segmentation - flexability - Security

⇒ VLAN Trunking:-

vlan Trunking types Frames Tagging with VLAN ID

[1] Inter switch Link [ISL] [30 byte]

- The Cisco proprietery trunking method that adds 26-byte header and 4-byte trailer on the original ethernet Frame.

ISL header (26 byte)	encapsulated ethernet Frame	CRC +4 byte

[2] IEEE 802 1q (Dot 1q)

- It is standard trunking method that isn't have only 4 byte field Tags to the original ethernet frame and recomputes the FCs

Dest	Src	tag	Len/etype	data	FCS
		↓ 4 byte			

← جميع بالافتراضي ports تكون موجوده في vlan 1 ويكون ارسال الداتا بين الاجهزه بدون Tag

Scanned with CamScanner

* Configuration An access LAN:-

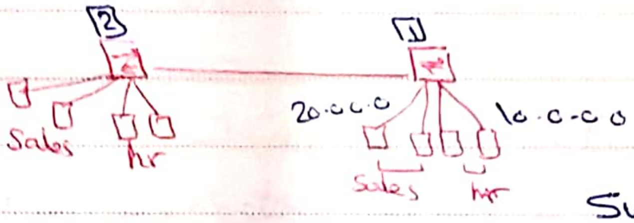
```
Switch (config) # vlan رقم الـ vlan
Switch(config-vlan) # name اسم الـ vlan
Switch (config) # int اسم المدخل
Switch (config-if) # switch port mode access
Switch ( config-if) # switch port access vlan رقم الـ vlan
```

← يتم تقسيم الاجهزة بحيث ان كل جهاز يتم توصيله بال port المحدد له

* Configuration A trunk LAN:-

```
Switch (config) # int رقم البورت الموصل للسويتش الاخر
Switch (config-if) # switch port mode trunk
```

Lab :-



Switch 2	Switch 1
#vlan 2	# vlan 2
#name hr	#name hr
#vlan 3	# vlan 3
#name sales	# name Sales
# int range fa/1 -10	# int range fa/1 - 10
# switch port mode access	# switch Port mode access
#switch port access vlan2	# switch port access vlan2
#int range go/11-20	# int range go/11-20.
#switch port mode access	# switch port mode access
#switch port access vlan3	#switch port access vlan 3
# int go/o	# Int go/o
#switch port mode trunk	# switch port mode trunk
#do wr	# do wr
#do show vlan brief	# do show vlan brief

← يتم اعطاء الاجهزه التابعه لل hr شبكة 10.0.0.0 والتابعه ل Sales
شبكة 20.0.0.0 وال hr ports من 1 حتى 10 وال Sales من 11 حتى 20
← عند ارسال رسالة من hr في Sw1 الى hr في Sw2 هتتم القراءة بينما
من hr الى Sales لا يتم القراءة

SENA

→ Inter vlan Routing with external Router 2

- RoAS = Routing as a stick

يتم توصيل الشبكة في النهاية بـ Router لتوصيل الجميع عن طريق كابل المدير عن طريق تقسيم Interface والسويتش يتحول Trunk

→ Configuration a Router 2

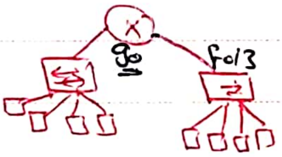
Router(Config)# In g0/0.2 ← 03 vlan حسب

encapsulation dot 1q 2 ← رقم الـ vlan

ip add IP mask

do wr

Lap



المثال السابق وهنضيف عليه Router

Router (2901)

Router(Config)# Int g0/0
#no shut down
#no Ip domain-lookup
int g0/0.2
#encapsulation dot 1q 2
#ip add 10.0.0.100 255.0.0.0
int g0/0.3
#. encapsulation dot 1q 3
ip add 20.0.0.100 255.0.0.0

switch

switch (config)# int fa0/3
#sw port mode trunk
#vlan 2
#vlan 3

← في كل pc يتم اضافة default gateway تبع الـ vlan

مثلا hr ← 10.0.0.100 Sales ← 20.0.0.100

← عند ارسال رسالة من SW1 لـ SW2 مش هيقراها الا من تاني مره

Scanned with CamSca

⇒ MIS [Multi layer switch] = layer 3 switch [mac+Ip]

يتم توصيل MIS للعمل كروتر حيث انه يفهم Ip و Mac حيث
انه يحتوي على روتر كـ S/W و ASIC يقوم بدون
الروتر ويقوم بتسجيل Routing table على H/W
وهذا يسمى FIB

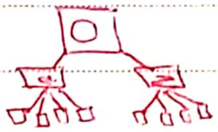


FIB → Forward Information Base

ويتم توصيله بالسويتش ولكن عدم عمل 2trunk مع بعض ويتم
استخدام #ip routing حتى يعمل كروتر

Lap

نفس المثال السابق مع وضع MIS مكان Router

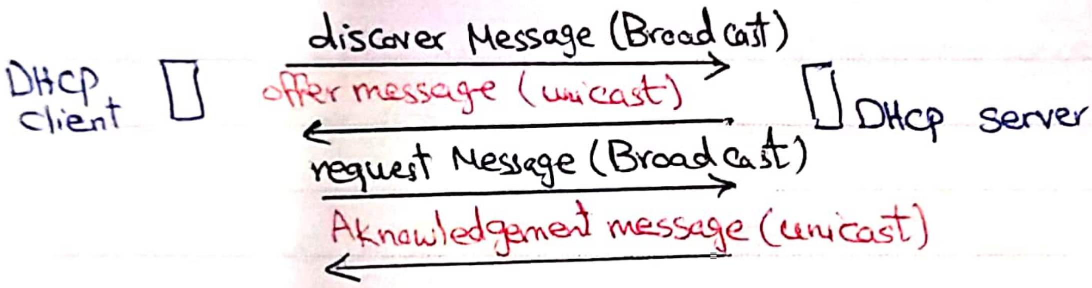


```
#vlan 2
#vlan 3
#int vlan 2
#ip address 10.0.0.100 255.0.0.0
#int vlan 3
#ip address 20.0.0.100 255.0.0.0
#ip routing
#do wr
#show Ip route
```

** DHCP [dynamic host Configuration protocol]

بروتوكول يستخدم لجعل ال Server يقوم بتوزيع Ip للاجهزة Automatic

→ DHCP reduce the complexity and amount of administrative network by using automatic Tcp/Ip Configuration



Manual Tcp/Ip Configuration	Automatic Tcp/Ip Configuration
• Ip addresses are entered Manually	• Ip addresses are supplied automatic
• Ip address could be entered Incorrectly	• Correct Configuration Information is ensured
• Communication and network issues can result	• client Configuration is updated automatically
• Frequent Computer moves increase administrative effort	• A Common source of network problem is eliminated

50 % at least duration has expired

رسالة تظهر عند وصول مدة ال dhcp ٥٠٪ من المدة

التاريخ: / / الموضوع

نفس الشبكة و لكن مش هندي PCs Ip انما هنشغل dhcp ونشارك Lap ٤
كل جهاز Ip عن طريق dhcp

```
Router(config)#int g0/0
#no shutdown
#Ip add 10.0.0.100 255.0.0.0
#int g0/1
#no shut down
#ip add 20.0.0.100 255.0.0.0
#do wr
#service dhcp
#Ip dhcp pool afaq
#network 10.0.0.0 255.0.0.0
#domain-name afaq.com
#default gateway 10.0.0.100
#dNS server 10.0.0.100
#ip excluded-address 10.0.0.0 10.0.0.50
#ip dhcp pool Asd
#network 20.0.0.0 255.0.0.0
#domain name asd
#default gateway 20.0.0.100
#dns server 20.0.0.100
#ip excluded-address 20.0.0.0 20.0.0.50
```

1. network
2. default gateway
3. DNS server
4. ip excluded-address

الاجهزة هنا خدت Ip عن طريق dhcp بطريقة Automatic ما عدا
من 0 حتى 50

* PVST = Peer vlan Spanning Treer

← تقسيم Switch الى Vlans بحيث يكون لكل Vlan ← Spanning tree
ليكون لكل Vlan ← root خاص به لتقليل الحمل على الكابلات
ومنع Loop

Loop
الشبكة المستخدمة دائماً

Switch [1]

(Config)# Spanning tree vlan 1 root primary

Switch [2]

(Config) # Spanning tree vlan 2 root primary

الموضوع   التاريخ: / /

Routing

* **Routed protocols:-**
That protocols that Carry data traffic from end to end
to provide ① Logical addressing
② encapsulation data from end to end

البروتوكولات المستخدمة لنقل البيانات من النهاية.

* **Routing protocols:-**
It is exchange of information between Routers so as each Router tell others about network it Can reach.

تبادل للمعلومات بين الروترز حيث أن كل روتر يبلغ الباقي بالشبكات الممكن الوصول لها.

* **Routing:-**

توصيل الروترات مع بعضها بحيث أن الشركة يكون لها أكثر من فرع

* To route the routing what reasons?

[1] destination addresses — معرفة العناوين البعيدة
[2] possible routes — يعرف الراوترز البعيدة المتاحة
[3] best route
[4] Maintain and verify routing Information — التعرف على افضل مسار

→ Identifying Static and dynamic Routes

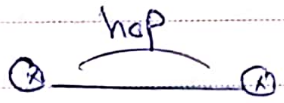
Static Routing اليدوي	dynamic routing اوتوماتيك
→ uses aroute that anetwork adminastrator entres into the router manually	→ uses aroute that anetwork routing protocols adjust automatically for topology traffic changes
→ build router table [routing table] manually	→ build routing table by Routing protocols
→ If network is simple	→ If network is complex معقدة
→ If one path exists to destination	→ If many paths exists to destination
	Routing protocols [RIP - ospf - EIGRP]

* الروتر يوجد بداخله Routing table تحتوي على المعلومات حول الشبكات المتاحة ويكون عن طريق Static or dynamic Routing

⟹ Static Routing:-

- Configure un indirect static routes to and from a stub network to allow Communication to occur يحدث

ده بيتم عن طريق تغيير اعدادات الروتر بحيث نجعل كل روتر يوصل للشبكة كذا عبر كذا عن طريق المدخل كذا



← التنقل من روتر للتاني يسمى next hop

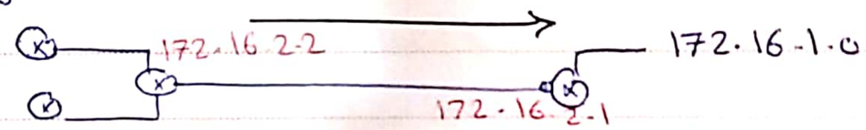
Static Routing method:-

(Config)# Ip route Network address Mask distance Interface

distance by default = 1

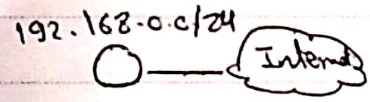
← الـ distance = metric = Hop

(ex)



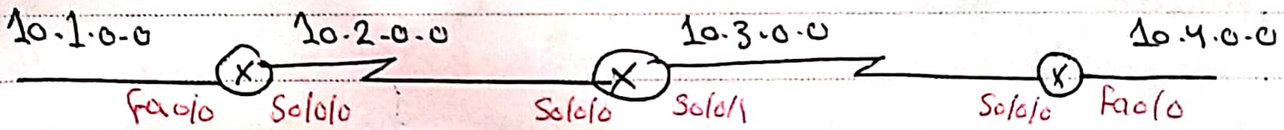
→ Ip route 172.16.1.0 255.255.255.0 172.16.2.1

(ex) Home Router



Ip route 0.0.0.0 0.0.0.0 Ip الروتر اللي هيوصلنا

(ex) Routing Table:-



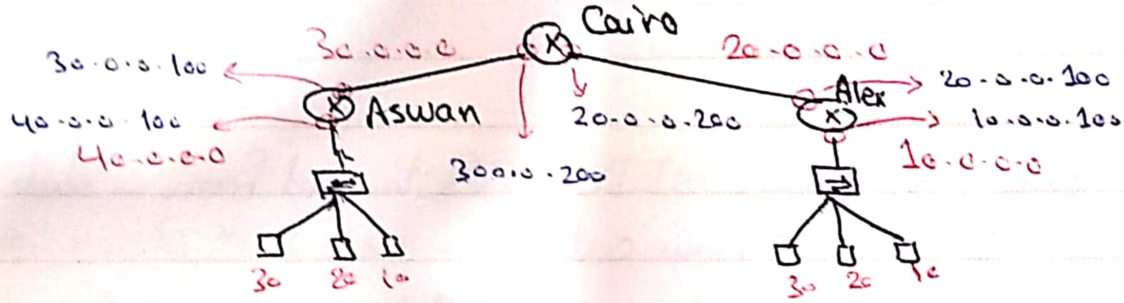
Network	Interface	metric
10.1.0.0	fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	1

Network	Interface	metric
10.1.0.0	S0/0/0	1
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	1

hop Count

Network	Interface	metric
10.1.0.0	fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Lap



← بعد تسطيب الشبكه و اعطاء كل Interface الشبكه الخاصه بها كما في الشكل الراوتر هتقرا بعض ولكن الاجهزه لا عملا الجهاز 10.0.0.10 مش هيقرا 40.0.0.10

← هيتم تسطيب Static route

→ Cairo

Cairo(Config)# ip route 10.0.0.0 255.0.0.0 20.0.0.100
ip route 40.0.0.0 255.0.0.0 30.0.0.100

→ Alex

Alex(Config)# ip route 30.0.0.0 255.0.0.0 20.0.0.200
ip route 40.0.0.0 255.0.0.0 20.0.0.200

→ Aswan

Aswan(Config)# ip route 20.0.0.0 255.0.0.0 30.0.0.200
ip route 10.0.0.0 255.0.0.0 30.0.0.200

Show Ip route

هيبين ايه المتصل بالروتر مباشرة وايه اللى تم توصيله Indirect

→ Automatic Routing :-

قيام الروتر بعمل Routing عن طريق ← Routing protocol

→ what is a routing protocol?

It is a protocol used between routers to determine paths and mantain.

· once the path is determined a router can routed protocol.

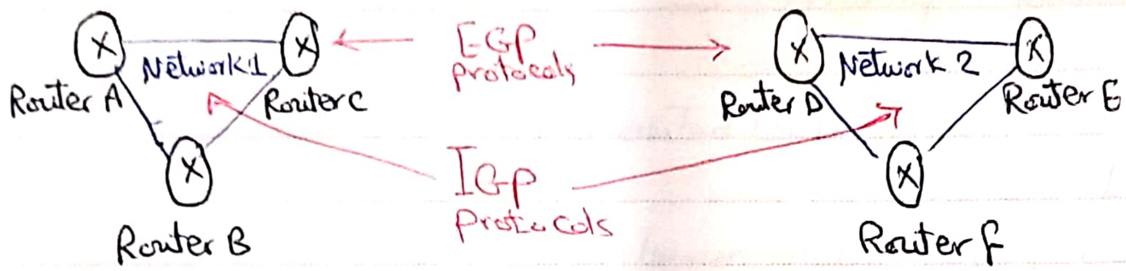
← يعني أن كل جهاز هيتم تسطيب عليه البروتوكول المستخدم [RIP - ospf - EIGRP] وهما هيتفاعلوا مع بعض ويعرفوا الشبكات.

Routing protocols types

- **IGPs** داخلي — Interior gateway protocols
  - distance vector
    - RIP1
    - RIP2
    - IGRP
    - EIGRP → Hybrid Routing
  - Link state
    - ISIS
    - ospf
- **EGPs** خارجي — exterior gateway protocols
  - ↓ path vector
  - ↓ BGP [Border gateway protocol]
    يقوم بربط Autonomous systems مع بعض

الانترنت عبارة عن مجموعات من Autonomous systems مربوطة مع بعضها كإيجيبت في Tedata والباقي.

* Exterior vs Interior Routing protocols *



→ The Routers within Network 1 are part of one autonomous system as are the routers in Network 2 within these networks we use IGP routing protocols whereas between these two autonomous systems, we use EGP routing protocols.

[1] RIP [routing information protocol]

→ distance vector _ How far vector which direction
بيعتمد على المسافه حيث انه بيختار الطريق الأقصر.
. سيتم تفعيل RIP على كل الاجهزه وكل جهاز بيرسل update
كل 30 sec لحد اقصى Max 180 sec
. بيعتمد على hop count = metric وهو عدد الروترات اللى هيعدى عليها
حتى يصل الى النهاية. metric → best path
→ distance vector _ source of information and discovering router

→ Administrative distance: choose best routing protocol
بيستخدم لاختيار افضل بروتوكول بحيث انه لو كل الروترات متسطبة على الجهاز
ومعظم [RIP _ ospf _ EIGRP] static هيختار static لانه ليه
اقل Administrative distance

Static → 1   RIP → 120   ospf → 110   EIGRP → 90

RIP Configuration:

Router (Config) # router rip → starts the RIP routing process
Router (Config_router) # network network number ← الشبكه المتصل بها

- Select participating attached Networks
- The network number must be a major classfull network number.

فى الاول امر بيغطى الروتر الشبكات اللى عايزينه يعرفها من الشبكات
البعيدة يعرفها من الروتر الاقرب ليه

Lap2

هستخدم نفس Topology بتاعت static ولكن هنلغي static عن طريق ومنع no قبل كل أمر كان مستخدم ---- # no ip route

Alex:- Alex(config)# router rip
Alex(config-router)# network 10.0.0.0
Alex(config-router)# network 20.0.0.0
do wr

Cairo:- Cairo(config)# router rip
Cairo(config-router)# network 20.0.0.0
Cairo(config-router)# network 30.0.0.0
do wr

Aswan:- Aswan(config)# router rip
Aswan(config-router)# network 30.0.0.0
Aswan(config-router)# network 40.0.0.0
do wr

show Ip route

هيوضح الشبكات المتصل بيها الروتر مباشر وامامها (C) و الشبكات المتصل بيها عن طريق RIP وامامها (R)

→ Symbol name in routing table is (R)

debug ip rip   هيظهر كل حاجه حصلت في ال rip

الموضوع   التاريخ: / /

** Maintaining Routing information problem _Routing Loops

← يحدث Loop للروتر بحيث انه يفصل عن روتر معين كان متصل بيه
بـ metric=0 ويقراه مره اخرى عن طريق روتر اخر بـ metric=2
اللى هو أساساً اللى معرفه عليه وبكده يحصل loop لأن الداتا
تفضل تلف وترجع لمصدرها مره اخرى

← لو حصل loop فى الشبكة فالنسبة لـ RIP ليه حد أقصى
لعدد hops وهو 16 وبعدها بيتوقف ويعطى Infailed

← والحل لهذه المشكلة هو Split horizon

Split horizon :- route learnt from Interface should never be advertisement on same Interface.

→ It is never useful to send information about a route back in the direction from which the original packet came.

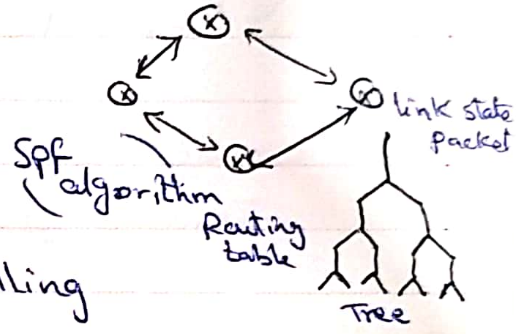
انه يمنع ارسال الـ update للجهة الرئيسية اللى بعتتها من البداية

* RIP V2 ⟶ # router rip   RIP version 2
version 2
network ____

RIP 1	RIP 2
→ classfull لا يفهم subnetting	→ classless
→ update Ip → broadcast 255.255.255.255	→ update Ip → Multicast 224.0.0.9
→ No authentication	→ Authentication → password
→ Receive RIP 2 data	→ not Receive RIP 1 data
يستطيع ان يتعامل مع الداتا المستخدمة فى RIP 2	

2 → ospf → [open shortest path first]

- link state routing protocol → بيعتمد على سرعة الخط
- steps



1. each router will send hello packet to all its interfaces to discover its direct connected neighbors.
2. each router will send LSA [link state advertisement] to all its neighbors, telling them about its LSA's
3. every router receive LSA packet will take copy of it and send it as it is to its neighbors.
4. each router will form a LSDB [link state data base] for all LSA's
5. each router will draw a link state tree and put it self as the root of the tree.
6. each router will apply SPF (shortest path first) Algorithm to get the routing table

- كل روتر هيبعت hello لجيرانه حتى يتعرف عليهم
- كل روتر هيبعت LSA للباقي ويتبادلوا LSAs والروتر اللي هيستلم ال LSA هياخد نسخة منها ويبعتها زي ما هي للتاني
- كل روتر هيكون LSDB وكل روتر هيرسم شجرة ويضع نفسه الأساس لهذه الشجرة
- كل روتر هيستخدم SPF Algorithm لكي يكون Routing table

→ ospf description:

1. Standard protocol
2. Classless protocol
3. Loop free topology — لا يوجد loop
4. Symbol name in routing table is "O"
5. Send packets on multicast address 224.0.0.5
6. Administrative distance = 110
7. Metric = Cost = 100 000 000 / Bandwidth $= \frac{10^8}{BW}$
8. Hop Count is unlimited [support hierarchical design] — غير محدود بالنسبة لعدد الروترات

→ ospf Configuration:

Router(config)# router ospf (Process ID)
Router (config-router)# network Direct Conneted Net ip wild Card mask area 0
area(0)

→ Process ID

- Locally Significant [1 – 65535]
- it is used to identify a unique instance of an ospf database

رقم يعبر عن الأولوية بحيث انه لو موجود مجموعة روترات الأقل هو الأول

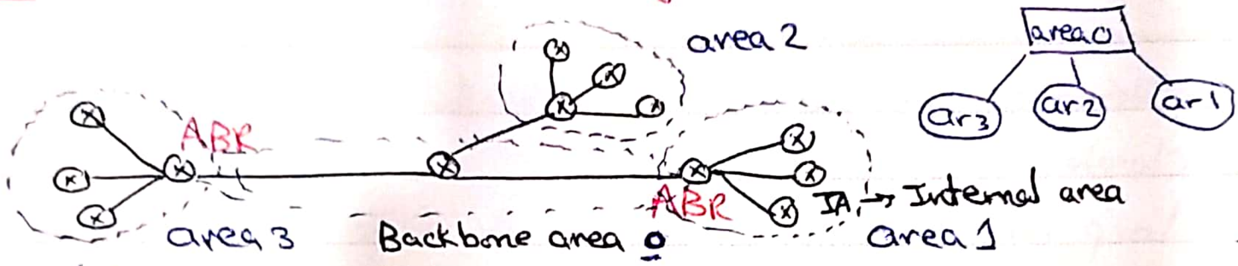
→ wild Card Mask [W-C-M]

- Inverted Subnet mask
- Continuous of 0's followed by Continuous of 1's
- wild Card mask = 255 – (subnet mask)

عبارة عن mask بالنسبة لـ host يعني الجزء اللي فيه host يبقا قيمته 256

والجزء اللي فيه network قيمته 0

→ Area : [Hierarchical design]



← عند زيادة عدد الروترات ولكل روتر database فعند زيادتها يؤدى الى زيادة الحمل على الروترات ويؤدى الى سقوطها فلذلك يتم استخدام hierarchical design لتقسيم الشبكة الى area

← كل الروترات متصل بـ BackBone Area 0

← الروتر اللى عالحدود اللى بيوصل الـ area بتاعته اسمه ABR [area border router]

ومهمته انه ياخد المعلومات من area ويوصلها للباقى

Lap: هنستخدم نفس Topology بتاعة الـ RIP ولكن بعد الغاؤه #no router rip

Alex:
```
Alex(config)# router ospf 1
Alex(config-router)# net 10.0.0.0 0.0.0.255 ar0
Alex(config-router)# net 20.0.0.0 0.0.0.255 ar0
```

Cairo:
```
Cairo(config) # router ospf 1
Cairo(config-router) # net 20.0.0.0 0.0.0.255 ar0
Cairo(config-router) # net 30.0.0.0 0.0.0.255 ar0
```

Aswan:
```
Aswan(config) # router ospf 1
Aswan(config-router) #net 30.0.0.0 0.0.0.255 ar0
Aswan(config-router) # net 40.0.0.0 0.0.0.255 ar0
                     # do show ip route
```

→ ospf Topologies :-

[1] BMA [Broad Cast Multiple Access]

ex:- Ethernet and token ring



التوصيل في الغالب بسويتش

→

[2] point to point :-

— A network that Joins asingle pair of routers

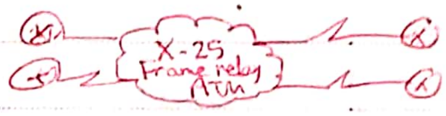


التوصيل بين روترين وهي المستخدمة في lab

ex:- Interfaces running PPP or HDLC or point to point Sub Interfaces ATM & Framerelay

[3] NBMA [Non broadcast multiple access]

- الروترات تتصل ببعضها عن طريق شبكة الانترنت الرئيسية ويتم تعيين روتر رئيسي لكي يتصل بابو بالتالي مفيش Broadcast ولكن هناك access



→ What is the importance of hierarchical design of ospf ?

① Minimize routing table entries

② Localizes the impact of atopology change within an area

→ Hello protocol :-

- Hello Interval every 10 sec

- Dead Interval every 40 sec

→ For routers to be neighbors :

- Must have the same [1] Area ID

[2] Hello and dead Interval

علشان الروترات تتصل مع بعضها لازم يكونوا في نفس الـ area

** Broadcast Multiple Access [BMA] Topology :-

- designated Router [DR] election
  DR Is the router with the highest
  1. ospf Priority [Default = 1 → 0 → 255]
  2. Router ID [RID]

• Router ID
1. Highest Loopback Interface on the router [virtual Interface]
2. Highest Active physical Interface on the router

← الروترات بتختار كبير لها وهو DR ويكون له في حالة الطوارئ BDR [backup designated router]

← يتم اختيار ال DR بناءً على Priority ويمكن تغييرها بهدف اختيار انسب روتر ويكون RID مماثل للـ IPV4 حتى يستطيع أن يتعامل معه والافضلية بعده تكون loopback Interface وهو وهمي نعمله ونديه اعلى Ip والتالي بعده physical Interface.

← ليه نعمل logical Interface طالما فيه physical Interface ؟

- لأن ال physical متصلة بالشبكة دائماً وقد يحدث بها كثير من السقوط فلذلك logical تكون أكثر استقراراً.

→ LSA are sent to DR and BDR on 224.0.0.6 and DR will take copy of it and resend it to everyone else on the segment on 224.0.0.5

- Problem:-
  Flapping Interface go up & down frequently, all routers will be busy for rebuilding (should) the tree

- Solution:-
  - To confine the network Instability, ospf support hierarchical level

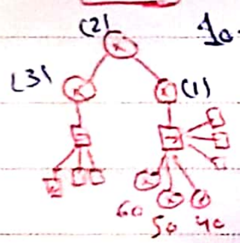
[1] Backbone area → area 0

[2] Regular area → area 1 = 4,294,967,295

- Multiple ospf area must be connected to area 0

Lap

Lap على تغيير الاولوية لاختيار DR



[1] ← هنستخدم نفس الـ Topology ولكن هنضيف للشبكه 10.0.0.0
٣ روترات ونعطى لكل منهم Ip وليكن
[10.0.0.40 _ 10.0.0.50 _ 10.0.0.60]
ونسطب ospf على كل روتر منهم

[2] ← عند كتابة الامر # show IP ospf neighbor
سنجد ان DR هو الروتر (1) لان له اعلى Ip وهو 20.0.0.100

1 التحكم في Priority

→ Router (Config)# Interface Fe/0 → المتصل بالشبكة
Router (Config-if)# ip ospf Priority number

Lap → # Int g0/0
ip ospf priority 5
do wr
show ip ospf neighbors

← نقوم بغلق الشبكة، وفتحها مرة أخرى عشان ميفضلش يبدل DR ومحصلش drop في الشبكة عشان Stability

← بعد كتابة الامر هنلاقي ان الروتر اللي ليه priority اعلى هو DR

2 التحكم في Loopback

→ Router(config)# Interface Loopback رقم
Router(Config-router)# ip address ip mask

Lap → # Int loopback 1
Ip add 60.0.0.50 255.0.0.0
do wr

لازم نقفل الشبكة الاول وبعد كده #show Ip ospf neighbors

[3] التحكم في Router ID

→ Router(config)# router ospf رقم
Router(config-router)# router ID IPv4 وهمية

[Lap]

router ospf 1
router ID 80.0.0.0
do wr

تسطيب area ←

من الممكن أن نغير area في كل روتر ولكن كلهم هيشوفوا بعضا عن طريق area 0.

[Lap]

Alex

#router ospf 1
#net 10.0.0.0 0.255.255.255 ar 1

Aswan

router ospf 1
net 10.0.0.0 0.255.255.255 ar 2

show Ip route

هنلاقي روتر Aswan شايف الشبكة 40.0.0.0 ولكن IA يعني Internal area يعني انه غير متصل بها direct ولكن هنا اعنا طريق Area 0 وكذلك روتر Alex شايف 10.0.0.0 كـ IA

3 EIGRP:-

→ EIGRP:- enhanced Interior gateway routing protocol
- Hyprid routing protocol

لحمد على الاستقرار

- EIGRP
1. Cisco proprietery protocol
2. classless protocol
3. Send packets on multicast address 224.0.0.10
4. Administrative distance=90
5. Fast Convergence use [Dual]
6. symbol name in routing table is "D"
7. Metric =Bandwidth & delay & Reliability & MTu
8. Max Hop Count =224

Advanced distance vector هو عدد رقم كبير في شبكة داخلية وممكن نقول عليه
انا انه RIP متطور

→ Hyprid Routing protocol:-
→ Support multiple Network Layer protocol [IP-IPX-Appletalk]

→ EIGRP Terminology:-
- Neighbor table → Table contain all neighbors
- Topology table → All routes to all networks
- Routing table → Best routes to all networks
- Successor(S) → Best route - feasible successor(FS) → Backup route
- Successor stored in the routing table & Topology table
  feasible successor [FS] stored in the topology table only

* Dual [Diffusion update Algorithm]

انتشار قاعدة

- This Algorithm stores a neighbor's routing information in all Topology table.
- If primary route in the routing table fails, Dual can take a backup path from the topology table and place in the routing table.
- If no backup route is found in the topology table, it will generate a query packet sent to the neighbors.

بكت استعلام

← كل الجيران موجودة في neighbor table ولكن اللي هيوصلوا موجودين في Topology table والافضل بينهم موجود في routing table - وهنا Dual هو تجميع كل البيانات عن الجيران ونقلها لـ Topology ولو حصلت مشكلة للروتر الرئيسي حيذهب لـ Topology table ويأخذ الاحتياطي لـ routing Table ولو مفيش يبعت استعلام لكل الجيران .

* EIGRP Configuration :

Router (Config) # router eigrp AS
Router (Config-router) # network direct connected net (Ip).

As → Autonomous system Number [1 – 65535]

وكل الروترات يجب ان يكون لها نفس AS

* EIGRP Troubleshooting :

→ Show Ip route
→ Show Ip eigrp neighbors
→ Show Ip protocols
→ Show Ip eigrp Topology
→ Show Ip eigrp Traffic
→ Show Ip eigrp interfaces

Lap

هنستخدم نفس ال Tology

Alex :- Alex(Config)# router eigrp 1
Alex(Config-router)#net 10.0.0.0
Alex(Config-router)#net 20.0.0.0
#do wr

Cairo :- Cairo(Config)# router eigrp 1
Cairo(config-router)# net 20.0.0.0
Cairo(config-router)#net 30.0.0.0

ASWAN:- Aswan(config)# router eigrp 1
Aswan(Config-router)# net 30.0.0.0
Aswan(Config-router)#net 40.0.0.0
#do wr

---

*By default, EIGRP automatically summarize subnets
Router (Config-router)# auto summary

ال eigrp يقوم افتراضيا بالتجميعات دي

→ This make EIGRP behave like a classfull routing protocol and therefore Summarize subnets on the classfull boundary
→ Automatic Summarization Can be disabled using the router Configuration Command.
#No auto-summary

← هناك مشكلة وهي انه كل روتر هيبعت classless و classfull باستخدام Summary فهيحصل Conflect عشان الروتر مش هيعرف التخيص جاي منين فلازم توقف auto summary

* EIGRP Composite Metric Calculation :-   حساب ال metric

- EIGRP Composite metric formula Consists of values K1 through K5 Know as EIGRP metric weights.
- By default, only K1 (Bandwidth) and K_3 (delay) are set to 1; K_2 (Load), K4 (Reliability) and K5 (MTU) are set to 0

يتكون من عناصر ولكن نعتمد على 2 فقط هم [Bandwidth + delay] وهم يعبرو عن السرعة

- K values Can be changed with the EIGRP router command

Router(Config-router)# metric weights tos K1 K2 K3 K4 K5

(K1 → Bandwidth, K2 → Load, K3 → delay, K4 → Reliability, K5 → MTU)

- Default Composite formula:-

metric = [K1 [Bandwidth] + K3 [delay]] = Bandwidth + delay

- Complete Composite formula:-

$$256 \times \left[K1 \times Bw + \frac{K_2 \times Bw}{256 - Load} + K3 \times Delay \right] \times \frac{K5}{REL \times K4}$$

حيث ان $K1 = K3 = 1$ و $K2 = K4 = K5 = 0$ من الشرح

$$256 \times [Bw + 0 + delay] \times 1 = 256 \times (Bw + delay)$$

SENA

Scanned with CamScanner

RIP	OSPF
[1] It is standard advanced distance vector [2] It send periodic update every 30 sec using multicast 224-0-0-9 [3] It sends update at change use split horizon	[1] It is open standard Link state [2] It send LSA using 224.0.0.5 و 224.0.0.6 [3] It send LSA at change and use split horizon
[4] It is classless protocol [5] optional Authentication password [6] use Ball manford Algorithm	[4] It is classless protocol [5] optional Authentication password [6] use dijestra Algorithm
[7] Symbol in routing table is [R] [8] Adminstrative distance = 120 [9] metric is hop max = 15	[7] Symbol in routing table is [O] [8] Adminstrative metric = 110 [9] Metric is cost $= \frac{10^8}{Bw}$
[10] support equal Load sharing [11] support auto Summerization	[10] support equal Load sharing [11] don't support auto Summerization but support Hierarchical design

EIGRP	BGP
[1] It is Cisco advanced distance vector	[1] It is BGP [exterior gateway protocol]
[2] It sends routing table using multicast 224.0.0.10	[2] It sends full table using unicast #router bgp AS #neighbor Ip of neighbor
[3] It sends partial update at change and use splitt horizon	[3] It send LSA at change and use splitt horizon
[4] It is classless protocol [5] optional Authentication password [6] use Dual Algorithm	[4] It is classless protocol [5] optional Authentication password [6] use BGP Algorithm
[7] Symbol in routing table is [D] [8] Administrative distance = 90 [9] metric is composite = 256 [Bw + delay]	[7] symbol in routing table is [B] [8] Administrative distance = 20 (out) _ 200 (in) [9] metric = 10 attributes
[10] support auto equal and not equal load sharing (Config)# router eigrp AS (Config-router)# variance [11] support auto summerization	[10] No Load sharing [11] Support auto Summerization

→ Router security:

- ACL = Access Control List   قائمة التحكم

عمل قائمة للتحكم في الشبكة ومعرفة الاجهزه تدخل على ايه وتمنع ايه
واول خطوة لعمل ACL يكون routing شغال وبعد كده نقوم
بعمل Control عليها

ACL Types

Standard

- filter data depend on src Ip only
  - numbered [1-99]
  - named
- * Std Acl should places as close as possible to destination
  [out] ← يكون اقرب للخروج

extended

- Filter data depend on
  1. src Ip
  2. dst Ip
  3. protocol
  4. Application
  - numbered [100-199]
  - named

→ In numbered Acl:
we cant delete a certain statement, only we can delete the whole Acl

→ In named Acl:
we can delete Certain statement Inside the Acl

* Acl are basically set of Commands that is grouped under Certain Name or Number to Control traffic flow.
  - Acl can do one of two Action [permit or deny]
    (permit ↓ يسمح, deny ↓ يمنع)
  - Acl Configuration على خطوتين
    1. Create Acl
    2. Apply Acl to a certain Interface

عبارة عن جمل تحت بعضها عبارة عن الامرين Permit و deny

- Maximum Number of Acl Can ~~can~~ be applied on each interface per protocol = 2
  [1 per direction] [1 inbound + 1 outbound]

  كل Interface بيكون عليه بروتوكولين فقط واحد داخل وواحد خارج

→ In an Inbound Acl:-
  packets are processed before they are routed to an outbound Interface.

→ In an outbound Acl:-
  packets are processed after they are routed to an outbound Interface.

* Statement are Processed from top to down

  يتم التعامل مع ال List من أعلى لأسفل

* once a match (تشابه) is found, No further statements are processed but if no match is found the packet will be dropped due to "implicit deny" "statement at the end of the List. Call "deny all"

SENA

→ At least, there is must be one permit statement in the Acl or other wise all packets will be dropped

يعني لو هفتح جهاز بنكتبه الأول وبعد كده باقي الشبكة لو فيه جهاز مش مكتوب في Acl هيتعمل له deny خلاص على الأقل يكون فيه سطر permit في Acl

→ In any Acl, we can't add statement between statements any new statement is added to the end of the list so the Sequence (الترتيب) is very important.

مينفعش نضيف بعد ما نخلص كتابة Acl

← يتم تحديد اتجاه الداتا In, out بالنسبه للروتر اللي هيتحكم في الدخول لانه لو اتعمل غلط مش هينفذ

* W-C-M [wild card mask]

class A	9	10	11	12	13	14	15	16
class B	17	18	19	20	21	22	23	24
class C	25	26	27	28	29	30	31	32
→	128	64	32	16	8	4	2	1
	128	192	224	240	248	252	254	255
عدد الاجهزة →	127	63	31	15	7	3	1	0

هو ال mask بالنسبه ل Host ويستخدم لمنع عدد من hosts

مثلاً لو عايز امنع ١٤ جهاز هيبقا الماسك 0.0.0.15

لو عايز امنع 30 جهاز 0.0.0.31 تبعاً لآخر سطر في الجدول

لو عايز جهاز واحد يبقا 0.0.0.0

→ Standard Acl ←

[1] Numbered :-

Standard Acl filter packets base only on Source Ip address In the packet header.

Configuration

[1] creation of Acl

(Config)# Access list [1-99] [permit/deny] Source Ip [Source w.c.m]

[2] Applying

(config)# Interface Interface name

(Config-if)# ip access-group [1→99] [In/out]

[2] Named :-

Configuration

[1] creation

(Config)# ip access-list standard Acl name

(Config-std nacl)# [permit/deny] Source Ip [src w.c.M]

[2] Applying

(Config)# Interface Interface name

(Config-If)# Ip access group Acl name [In/out]

Lap std.numbered

← هنستخدم نفس الـ Toplogy لو عايز امنع اول
٢٠ جهاز من الشبكة 40.0.0.0 للوصول الى الشبكة
10.0.0.0

Alex → (Alex)(Config)# Access_list 1 deny 40.0.0.0 0.0.0.31
Access_list permit any   السماح للباقي
interface g0/0
Ip Access_group 1 out
do wr   تكون out عند الشبكة فقط
لانها لو In هتمنعها عن الشبكة كلها.

Lap std-named

(Config)# ip access_list standard Asd
Permit host 1.2.3.4
deny host 5.4.3.6
do show Access_list

standard Ip access list asd
10 permit host 1.2.3.4
20 deny host 5.4.3.6

(Config-std nacl)# 15 permit 8.5.4.2   هيضيفه للـ list
do show access_list

standard Ip access list asd
10 permit host 1.2.3.4
15 permit host 8.5.4.2
20 deny host 5.4.3.6

→ extended Acl ←

→ It is more flexible than Standard Acl
extend Acl can match on

1. Source Ip and destination Ip — يسمح بكل حاجه [Browse - download]
2. Tcp/Ip protocols [TCP (Browse eq 80), UDP, ICMP (ping), Ip (→ network layer)]
3. protocol Information [port number ICMP message type]

1. Numbered:-

*extended Acl should be placed as close as possible source.

Configuration

1. Creation

(Config)#Access-list (100-199) (permit/deny) Tcp/Ip protocol Source Ip src w.c.M destination Ip dst w.c.M [operator + destination protocol Information]

operator → eq = equal lt → less than or equal
gt = greater than or equal

protocol Information → Port Number

2. Applying

(Config)# Interface Interface name
((Config-if) # ip access-group [100 → 199] [In, out]

2 Named:

Configuration:

1 Creation

(Config)# ip access_list [extended] Acl name

(Config-ext-nacl)# (permit/deny) TCP/IP protocol Source Ip (Src w.c.m) [operator + Source protocol information) destination Ip (destination w.c.m) [operator + destination protocol Information]

2 Applying

(Config)# Interface Interface name

(Config-if)# ip access_group [Acl Name] [In/out]

Lap ext-numbered

هنضيف server وندية Ip ← 10.0.0.60 هنخلي اول ٣٠ host في 40.0.0.0 ميعرفوش يتصفحوا وتاني ٣٠ يعملوا Browse و ping للسيرفر

Aswan(Config)# access-list 100 per ICMP 40.0.0.0 0.0.0.31 host 10.0.0.60

Access List 100 deny Ip 40.0.0.0 0.0.0.31 any

Access-list 100 per TCP 40.0.0.32 0.0.0.31 host 10.0.0.60 Eq 80

access_list 100 deny Ip 40.0.0.32 0.0.0.31 any

access_list 100 per Ip any any

int g0/0

Ip access_group 100 In → اقرب الـ src

** Telnet :

Restricting Telnet Access to the Router Configuration

(Config)# Line vty 0 4
(Config-line)# access-class [1 → 99] [in/out]

Lap

عايز 10.0.0.20 هو بس اللي يقدر يدخل على الأجهزة

Aswan (Config)# enable password 123
Line VTy 0 4
Aswan (config-line)# Password asd
Login
access-list 1 permit host 10.0.0.20
line VTy
Access-List 1 in

WAN
[wide area Network]



توصيل WAN على مستوى العالم عن طريق

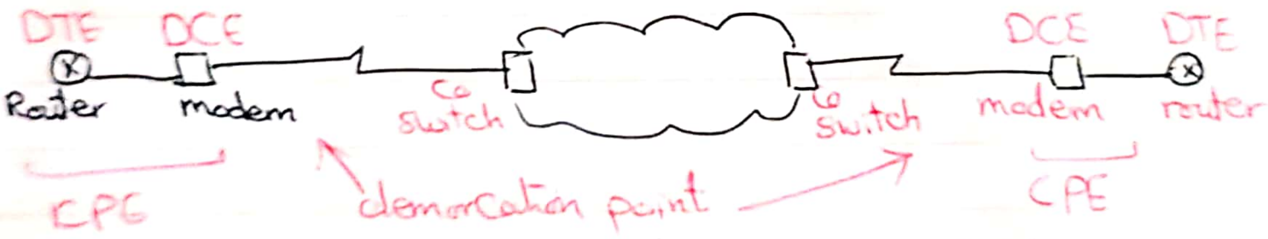
Isp → Internet service provider

لكي يتم ربط الروترات ببعضها وهذا عن طريق VPN

VPN → virtual private network

وهو يستخدم خاصية تسمى Tunnel

• WAN overview :-



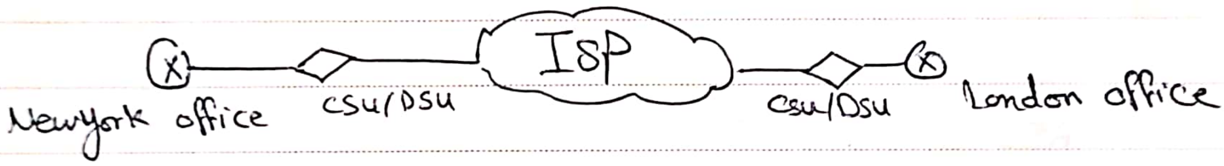
فالبيت احنا شغالين على DSL

• WAN Connection types
1. leased Line
2. circuit switched
3. packet switched
4. ATM

• WAN encapsulation protocols
- ATM
- HDlC
- PPP
- Frame Relay

[1] leased Line:- الخط المتأجر

- The link is available all the time with all dedicated band width الخط متاح طول الوقت بسرعة مش بتقل زى ما عندنا فاليست لعدد العملاء
- No Call setup procedure before transmitting data.
- only support point to point Connection
- expensive [fixed Cost] بتدفع ايجارها حتى لو مش هستخدمها



[2] Circuit switching:-

- The link is available but only for the duration of Call
- need Call setup procedure before transmitting data
- only support point to point Connection
- cheaper when Connectivity is not all the time [variable cost]
- useful for backup Connection
- example [1] Analog Dial-up Connection [modem]
  [2] Digital Dial-up Connection [ISDN]

protocols → HDlc - PPP

[3] Packet Switching:-

- The router is connected to TelCo [Telephone Company] using a single physical line with the possibility of being able to forward traffic to all of other sites.
- Support point to multipoint connection [Virtual Circuit]
  example Frame Relay [FR] → Delci

[4] ATM [ASynchronous Transfer mode]

- ATm and using Cell switching
- Speed = 40 Gbps

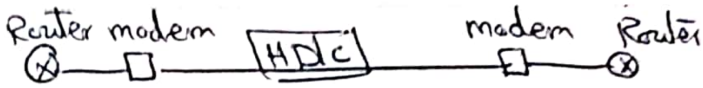
→ public WAN Broad Band [DSL] → digital subscriber line

- It is using all available frequency to gain higher speed
→ ADSL [ASymmetric digital subscriber Line]
- home user   - download > upload

→ SDsl [Symmetric digital Subscriber Line]
- enterprise using   - download = upload

** HDLC [highlevel datalink Control protocol]

- It is the default encapsulation on serial Interfaces of Cisco routers.
  هو الافتراضي بالنسبة لسيسكو على ال Serial
- per vendor protocol
- Has no options



- Configuration → Router(config-if)# encapsulation HDLC

→ ISO HDLC

Flag	address	Control	data	FCS	Flag

FCS → Frame check sequence

• Not support on Cisco devices

→ Cisco HDLC

Flag	address	Control	proprietary	data	FCS	Flag

proprietary → Type [IPv4 – IPv6]

** PPP [Point _ to _ Point protocol]

- It is a standard protocol



- PPP options

1. Compression
2. Call back
3. multi_link
4. Authentication [PAP – CHAP]
5. using LCP [Link control protocol] for Hello Packet
5. Configuration → (config-if) # encapsulation PPP

* PPP Authentication protocols:-

[1] PAP [ppp authentication protocol]

username	password
—	—

وده بسيطه بيكون فيها username و password فقط

(config)# username ______ password ______

[2] CHAP [Chalenge handshake authentication protocol]

username	password	Process id	random
—	—	ترتيبي	عشوائي

← وده معقد بيطلب فيه أكتر من شئ ويكون مشفر

ويطلب فيه ٤ أشياء [username+password+Process id + random no]

ويتم التعامل معه باستخدام MD5 ← message digest 5

→ enable ppp encapsulation

Router x (config-if)#encapsulation ppp

→ enable PAP or CHAP authentication

Router X(config-if)# ppp authentication [chAP /CHAP PAP /PAPCHAP/PAP]

Flag	address	Control	protocol	FCS	data	Flag

- PPP Can Carry packets from Several protocol suites using NCP
- PPP Controls the setup of sever Link options using LCP [Link Control protocol]

** Frame relay [FR]

→ Frame relay is data link Layer [Layer 2]

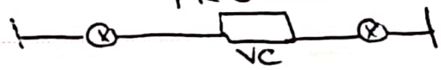
- Frame relay is apacket switching technology
- FR support multiple access technology depending on the Concept of virtual circuit [VC]
- Virtual Circuit → Is alogical connection between 2 devices

PVC → permanent virtual circuit = micro segments



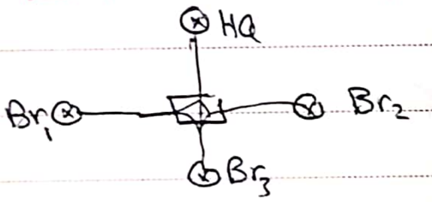
* Frame Relay Topologies:-

[1] point to point



← يتكون دائرة افتراضية للتوصيل VC تمثل كيبل

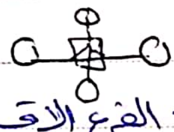
[2] Full mesh Topology:-



يوجد اتصالات مع جميع الفروع

no. of pvc $= \frac{n(n-1)}{2} = \frac{4 \times 3}{2} = 6$ pvc

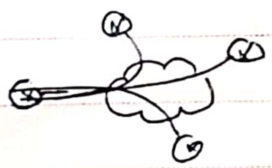
[3] partial mesh Topology:



جزئي

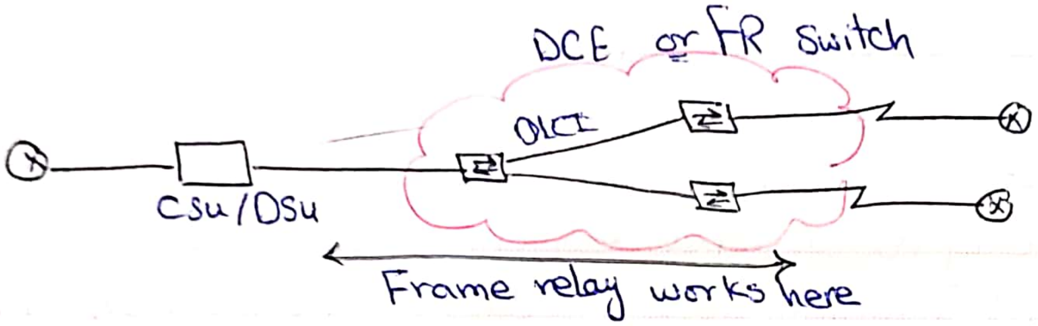
← لا يتم فيها الاتصال مع الفرع الاقل استخداما

[4] star [Hub and spoke]



يتم استخدام روتر رئيسي للجميع

→ Frame Relay by default is NBMA



← FR مش هيشتغل mac address انما بيشتغل DLCI وبيستخدم RARP لكي يتعرف على Ip address من خلال DLCI

DLCI → data Link Connection Identifier

- each VC has a unique Local address Called DLCI
- DLCI is Locally significant

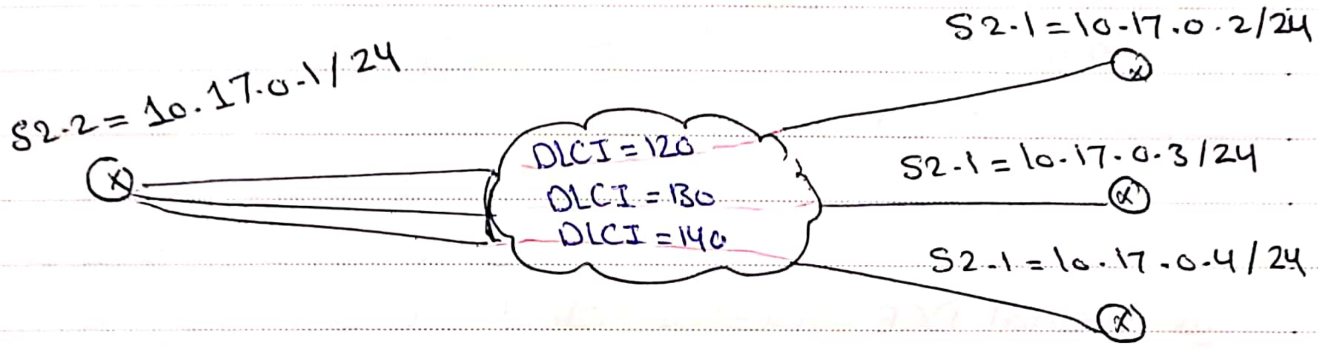
وبيستخدم LMI علشان يعرف هل الخط active or Inactive

LMI → Local Management Interface :-

- Signaling protocol between Router and FR Switch [keep alive & VC status]
- LMI is locally significant

* LMI types →
  1. Cisco [default on cisco devices]
  2. Q 933a (standard)
  3. AnsI (American)

→ Configuration Frame relay Multipoint Sub Interfaces :



- Interface Serial 12
- no Ip address
- encapsulation Frame relay
- Interface Serial 2.2 multipoint
- Ip address 10.17.0.1 255.255.255.0
- band width 64
  - Frame relay map ip 10.17.0.2 120 broadcast.
  - Frame relay map ip 10.17.0.3 130 broadcast.
  - Frame relay mip ip 10.17.0.4 140 broadcast

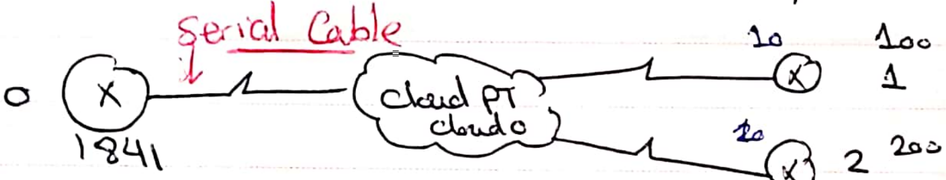
يتم تحديد كل DLCI هيوصل لفين عن طريق RARP
ويتم تحديد السرعه (clock rate) من قبل ISP [DCE] ويتم تطبيقها على الروتر (DTE).

→ [Configuration a serial Interface]

1. enter global Configuration mode → Router # Configure Terminal
2. specify Interface → Router(Config)# Interface S0/0/0
3. set clock rate on DCE Interface only
   Router(Config-if) # Clock rate 64000

Lap

سيتم استخدام Star [Hub and spoke]



← الروتر المستخدم 1841 لا يحتوى على Serial Interface فسنقوم
بإغلاقه ونضيف في اى وكايه ظاهريه WIC-2T
← الكابل المستخدم Serial Cable يتم اختياره تبعاً للبدايه اذا كانت
بدايه توصيل الكابل بـ cloud نستخدم Serial DCE بينما
اذا كان سنبدأ بالروتر نستخدم Serial DTE

Cloud

← تعطى للروتر R1 → 100 و R2 → 200
المطلوب في cloud هو تسطيب ان DLCI 100 تصل لروتر 1
و DLCI 200 تصل لروتر 2
← ندخل للاعدادات Config وسطيب

Serial 0 —add→ dlCI 100 - dlCI 200
serial 1 → dlCI 100
serial 2 → dlCI 200

← هنروح لـ Frame relay من الاعدادات ونختار

Serial 0 —add→ DLCI 100 → Serial 1
Serial 0 —add→ DLCI 200 → Serial 2

بالنسبه للروتر يمكن اعداد الـ Interface من Config ومن العكس
عن طريق CLI ← التسطيب العادى

الموضوع   التاريخ: /   /

Router 0

```
# Int S0/0/0
#no shut down
# clock rate 8000
# encapsulation Frame-relay
# Frame-relay Interface-dlCI 100
# Frame-relay Interface-dlCI 200
# Ip add 10.0.0.1 255.0.0.0
```

Router 1

```
#int S0/0/0
# no shut down
# clock rate 8000
# encapsulation Frame-relay
# Frame-relay Int dlci 100
# ip add 10.0.0.2 255.0.0.0
```

Router 2

```
# int S0/0/0
# no shut down
# clock rate 2000
# encapsulation Frame-relay
# Frame-relay Interface-DLCI 200
# Ip add 10.0.0.3 255.0.0.0
```

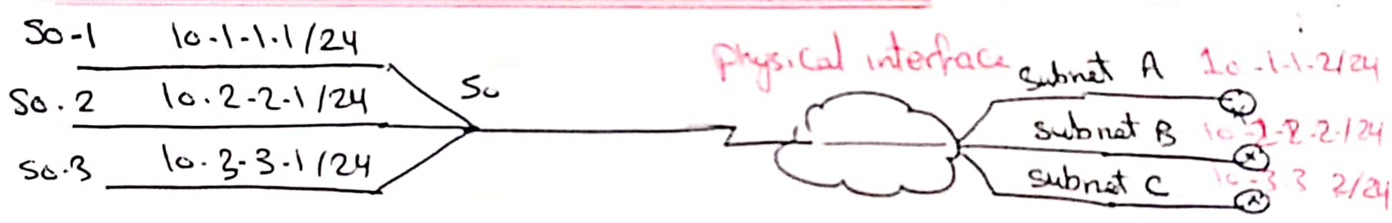
سجد أنا الروتر 1 شايف 0 اما 1 لا يرى 2 وهذا المشكلة وجود routing

SENA

← لو عايزين نعمل routing ـ

احنا بنستخدم NBMA يعني لو عايز يتكلم يروح للرئيسي وهو يوصلــه
ويسجل في routing table فإذا كنا عايزين نعمل routing هيطلعلي
Split horizon ودة هيسبب مشاكل RIP مش هيقدر يشتغل
بينما ospf و EIGRP عادي .

→ Resolving NBMA Reachability Issues



Split horizon Can Cause problems In NBMA environment :-

[1] Solution :- Sub Interfaces

[2] A single physical Interface simulate multiple logical Interfaces

يتم تقسيم الـ Interface الى اكثر من واحد بحيث كل واحد فرعي يوصل لشبكه

Lap **Router 0**

```
# no Frame-relay Interface dlCI 100
# no Frame-relay Interface dlCI 200
# int S0/0/0.1
# no Ip add
# Frame-relay Interface-dlCI 100
# ip add 10.0.0.1 255.0.0.0
```

التاريخ: / / الموضوع

Int s0/0/0.2 point to point
Frame-relay Interface-DLCI 200
Ip add 20.0.0.3 255.0.0.0
router rip
net 10.0.0.0
net 20.0.0.0

سيتم تغيير الشبكة في R2 الى 20.0.0.3

router 1 | # router rip
network 10.0.0.0

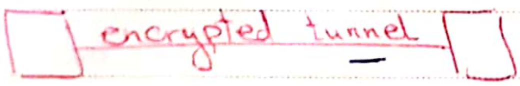
Router 2 | # router rip
network 20.0.0.0

#show Ip route

. VPN [virtual private network]

→ use WAN to connect private network

شبكة افتراضية وهمية خاصة تعمل على توصيل الطرفين في سرية تامة
وهذا عن طريق Tunnel



. Importance of VPN
1. Confidentiality
2. authentication
3. Integrity
4. anti reply

- VPN types
1. GRE
2. Ip sec
3. SSTp

MD5 → message digest 5 [128 bit]
SHA → Secure hashing Algorithm [512 bit]

Lab — سيتم استخدام GRE Tunnel ويتم تطبيقه على نفس الـ Topology

router 1 — يتم تحديد src و dst

```
(Config)# int tunnel 1
  # ip add 50.0.0.1 255.0.0.0
  # tunnel Source S0/0/0
  # tunnel dst 20.0.0.3
```

Router 2

```
(config)# int tunnel 1
  # ip add 50.0.0.2 255.0.0.0
  # tunnel Source S0/0/0
  # tunnel dst 10.0.0.1
```

Show Ip route

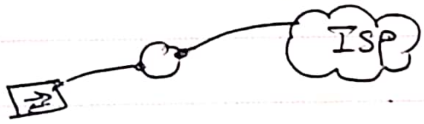
ستجد أن الروترين شايفين الشبكة 50 S c يعني direct

** Address Space Management :-

Scaling the network

NAT [Network address translation]

يستخدم لتحويل private Ip الى public Ip للخروج من الانترنت
كل جهاز يكون له private Ip يستخدم في LAN فقط ولكن عند خروجه للـ WAN
يأخذ public Ip وهذا يكون عن طريق NAT



[1] Static NAT :-   يدوي

- used for servers   يتم وضعه يدويا للشبكات المعروفه الثابته مثل السيرفرات

static Configuration :-

[1] Establishes state Translation between an inside Local address and Inside global address.

Router(Config)# Ip nat inside source static local Ip global Ip

[2] Marks the Interface as Connected to the inside   اختيار الداخلي In

Router(Config)# int g0/0
Router(Config-if)# ip nat inside

[3] Marks the Interface as Connected to the outside   اختيار الخارجي

Router(config)# int g0/1
Router(Config-if)# ip nat outside

[3] Display Active Translations :-

Router # show Ip nat translations

Lap هنستخدم نفس الـ Toplogy المستخدم فى Static routing وكده In و out

Alex → Alex(conf)# int Fo/0
Alex(conf-if)# ip nat inside
int Fo/1
ip nat out side
ip nat inside source static
10.0.0.20   20.0.0.20
do wr
show Ip nat translation

هيظهر الـ Ip الاساسيه الـ public Ip اللى خارج بيه الجهاز

2 dynamic NAT:-

- used for users

يتم اعطاء الجهاز Ip وهو يقوم بتوزيعها على الاجهزه فمثلاً لو عندى 10 IPs وكنا محتاجين نضيف جهاز أخر لنا يجد Ip .

- dynamic Configuration:

1 Defines a pool of global addresses to be allocated as-needed
Router (Config)# ip nat pool Pool name start Ip end Ip
net mask mask

[2] Defines a standard Ip ACL permitting those inside local addresses that are to be translated.

Router(Config)# access_list access list number permit source src w.c.M

[3] Establishes dynamic source Translation specifying the ACL that was defined in the previous step.

Router(Config)#ip nat inside source list access_list number pool name

[4] display Active Translations:

Router(Config)# Show Ip nat translations

(Lap) هستخدم نفس ال Toplogy مع الفاصل Static nat وخلي out و In كما هي

Alex → Alex(Config)#no ip nat inside source 10.0.0.20 20.0.0.20

Alex(Config)# ip nat pool asd 20.0.0.30 20.0.0.40 net mask 255.0.0.0

access_list 1 permit any

#ip nat inside source list 1 pool asd

do show Ip nat translation

هلاقي كل جهاز هياخد Public Ip للخروج

الموضوع   التاريخ: / /

[3] PAT [port address translation]

← هو المستخدم في البيت ودة معناه أن كل الاجهزة هتخرج بـ Ip الخاص بالروتر وعند العودة ترجع للروتر وهو يقوم بتوزيعها تبعاً للـ port ودة بيكون باستخدام Socket

Socket = Ip + port number

← port هو الرقم المستخدم من Tcp أو UDP في Transfir المستخدم وهي تكون من [1024 → 65535]

PAT Configuration

[1] defines a standard Ip Acl that will permit the Inside Local addresses that are to be translated

Router(Config)# access_list access list name permit source src w c m

[2] Stablishes dynamic source translation specifying the AcL that was defined in the previous step

Router(Config)# ip nat inside source list access list number Interface Interface overload

[3] display Active Translation

Router(Config)# do show Ip nat translation

Lap Pool asd ⟶ Int fo/o overload نفس السابق ولكن سيتم استبدال

Alex(config)# ip nat pool asd 20.0.0.30 20.0.0.40 netmask 255.0.0.0
acc 1 per any
ip nat inside source list 1 Int fo/0 overload
do show Ip nat translation

عليه يتم استخدام [dynamic + PAT] معاً اي يتم اضافه overload في الاخر

ip nat inside source list 1 pool asd overload

* Cable virtualization:-

EC → ethernet channel   تجميع الكابلات

→ It is merging many physical cables to act as Logical cable.

→ EC channel benefits:-

[1] Logical grouping of many physical ports
[2] Load distributions [Increase BW][speed]
[3] Link level redundancy الاستبدال [Active _Backup]

← القيام بتجميع مجموعة من البورتات للعمل كمجموعة واحدة ويقوموا بنقل الـ data فبالتالى هيتم تقسيم الداتا عليهم مما سيؤدى الى زيادة السرعة.

الشروط للقيام بهذا.

[1] يكون لهم نفس السرعة
[2] يكون عدد البورتات [2 - 4 - 8 - 16 - 32] لكى يتم توزيع عليهم

* This can be done by EC protocols
[1] PAGP = port aggregation protocol [Cisco only]
[2] LACP = Link aggregation control protocol [Standard]



فلاحظ انه هيشغل port واحد ويوقف ٣

لكل سويتش

```
switch(config)# Int rang fo/1-4
# Channel group 1 mode on
# Show ethernet channel
```

من الممكن ان اختار مكان on ← [PAGP - LACP] وهنلاحظ ان كل البورتات هتشتغل

* Remote Access to switch

القيام بالتحكم بالسويتش وعمل Telnet عن بعد

[Lap]   [⇄] ———— [PC] هيدخل على الـ Interface الخاصة بـ Vlan الموجود عليها جهاز PC

[Switch]

```
Switch(Config)# int vl 1
switch(Config-if)# no shutdown
                  # ip add 10.0.0.100 255.0.0.0
                  # exit
Switch(Config)# Line VTy 0 4
Switch(Config-line)# password 555
                  # login
                  # enable password 123
                  # do wr
```

[PC] > Telnet 10.0.0.100

هيطلب الـ password الخاص بـ Line و enable

* High availability [H.A]



← عند توصيل الاجهزة على روتر معين قد يهدد ال Stability وجود هذا الروتر فإذا سقط لن يستطيع الجهاز الوصول الى ال WAN فلحل هذه المشكلة سيتم عمل Virtual Router ليه Ip واحد

→ Virtual Router :-

- It is merge many physical routers to act as one virtual router have one virtual mac address and one virtual Ip by protocols

→ High Availability :-

تعتمد على طريقتين

Fail over	Load Balancy
واحد Active وواحد Backup	الاثنين Active و تقسيم الحمل

→ H A protocols :-

[1] HSRP = Hot standby router redundancy protocol

↳ Cisco only

← المستخدم وهو يعتمد على Failover

ويتم اختيار ال Active و Backup عن طريق

[1] priority

[2] The high Ip become active — لو ال priority متساوية

[3] Hello message 5 → 15 sec

[2] VRRP = virtual router redundancy protocol

ده Standard وخاص بـ IEEE ويعتمد على Failover

[3] GLBP = Gateway Load balancy protocol

وده بيعتمد على Load balancy L> Cisco

- Single virtual Ip address and multiple mac address
- traffic to single gateway distributed across routers.
- Automatic rerouting In the event of any failure
- depend on Load balancy

← الذي يحدث هو عند سقوط Active ينتظر الـ Backup الـ hello اذا تأخرت عن 15sec يصبح الـ Backup هو Active و الـ listeners هم Backup

Lap



عند انقطاع 10.0.0.100 لن يستطيع الجهاز 10 من الخروج الى WAN
اذا كان default gateway هو 10.0.0.100 ولكن الحل
هو جعل default gateway لجميع الـ PCs هو 10.0.0.150 مثلاً
كـ Ip لـ virtual Router

Router 1 - Router 2

Stand by [1-255] Ip 10.0.0.150

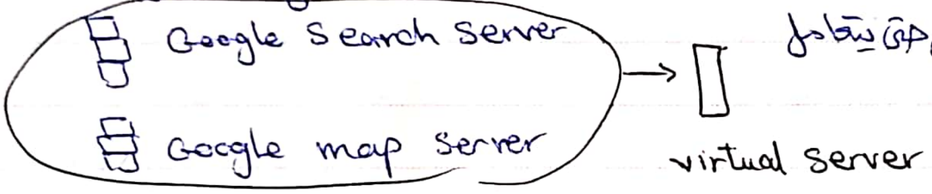
PCs → default gateway 10.0.0.150

Show standby

ستجد أن كل الاجهزه سوف تتصل عن طريق هذا virtual router!

* Server virtualization

- Merge many server to act as one virtual server



تجميع اكثر من سيرفر حتى يتعامل كسيرفر واحد

* virtual machine [VM]

- divide main server into sub servers to save resources

Banners

قد يوجد اكثر من فرع للشركة والمطلوب وضع رسائل في بداية الروتر لمعرفة هو تابع لفرع ايه

Lap

Router(config)# banner

banner motd ? # ________

________ #

do wr

تكتب رسالة الترحيب بين رمزين من نفس النوع وعند الدخول للروتر في وضع user سوف تظهر هذه الرسالة.

⇒ Security Enhancement :-

1. Port Security Scenario 1

- An attacker enables a hacking tool on the attacker's rogue device to flood switch mac tables with bogus MAC addresses, causing the MAC address table to fill up. When the MAC address table is full it turns the switch into a hub and floods all unicast frames.

هجوم على السويتش ويقوم بالارسال لل switch كل ثانيه حتى يحدث Flood
ويحوله ك Hub وهنا يستطيع أن يأخذ نسخة من البيانات
ومن البرامج التي قد تفعل ذلك Marcov + switch snipper

2. Port Security Scenario 2

- Port security is configured on untrusted user ports. Enabling port security limits MAC flooding attacks and locks down the port.
- Port security also sets an SNMP trap alerting of any violation. Port security allows the frames from already secured MAC address below the maximum number of MAC addresses enabled on that port. And any frame with a new mac address over the limit of dropped.

حماية الشبكه اذا تم تغيير MAC بتاع الـ port لو غيــــر غير كابل
الشبكه من جهاز لجهاز يتم التحكم في port ويمكن غلقها وهى أن
كل بورت مسجل على الشبكة بـ MAC معين عند تغيير هذا
الماك يغلق الـ port.

** Configuring Port Security:-

1. step 1: Enable port security
   Switch (Config-if) # switch port port-security
2. step 2 :- Set a maximum number of MAC addresses that will be allowed on this port. the default is one :-
   Switch (Config-if) # switchport port-security Maximum value
3. step 3 :- Specify which MAC addresses will be allowed on this port (optional):-
   Switch (Config-if) # Switch port port-security mac address
   نكتب ← mac address or sticky ← يقوم بتسجيل mac automatic
4. step 4 :- Define what Action an Interface will take if a non allowed MAC address attempts access.
   switch (Config-if) # Switchport Port-security violation [shutdown - restrict - protect]

Shut down → اغلاق البورت نهائياً ولا يفتح الا اذا تم عمل shutdown ثم no shut down

restrict → سوف يخبرك بأن هنالك تغيير في البورتات

protect → يقوم بالتوقف عند تغيير MAC address ولكن عند العودة الى الجهاز القديم يفتح عادي

Lap

سوف يتم تكوين شبكة من Switch وعدد اجهزة
يكونوا لها نفس الشبكة وليكن 10.0.0.0



Switch

```
Switch(config)# interface range fo/1-24
switch(config-if)# switchport port-security
# switch port mode access
# switch port port-security
  mac-adress sticky
# sw port-security violation
  shutdown
# do wr
```

← سيقوم الـ Switch بقراءة كل port وحفظ الـ MAC address الخاص به
وعند القيام باضافة جهاز جديد واعطاءه Ip address تبع الشبكة
واخذ كابل من احد الاجهزة له سوف يتوقف الـ port
حتى عند اعادة الـ Cable لنفس الجهاز اللي كان عليه
← حتى يعمل الـ port مرة اخرى نقوم بعمل Shutdown ثم
no shutdown

* NDP [Neighber discovery protocols]

[1] CDP [cisco discovery protocol]

* Configuring CDP
  - CDP is enabled by default
  - disable CDP
    [1] globally → # no cdp run
    [2] on an Interface → # no cdp enable
* Displaying CDP :-
  - # show cdp neighbors
    - show which devices are seen on which ports.
    يظهر المتصلين بالبورتات

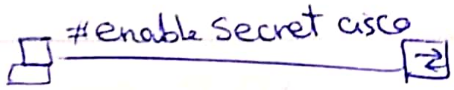
[2] LLDP [Link layer discovery protocol]

* Configuration LLDP :-
  - LLDP is disabled by default
  - enable LLDP
    [1] globally → # lldp run
    [2] on an Interface → # lldp enable
* Displaying LLDP :-
  - # show lldp neighbor
    - displays a summary of devices are seen on which ports.

* Securing Switch Access:-

[1] Telnet vulnerabilities:- (نقاط الضعف) — غير امن بما فيه الكفاية

- All usernames, passwords, and data sent over the public network in clear text are vulnerable.
- A user with an account on the system could gain elevated privileges.
- A remote attacker could crash the Telnet Service preventing legitimate use of that service by performing a DoS attack such as opening too many bogus Telnet sessions.
- A remote attacker can find an enabled guest account that might be present anywhere within the trusted domains of the server.



- الـ Telnet فيه مشكلة وهي ان كل الاسماء والباسوردات والداتا ممكن ارسالها عبر الانترنت من خلال Text ويكون ضعيف
- اي عميل على الشبكة قد تكون له امتيازات كثيرة والباحث او الداخل من الممكن ان يتحكم الـ Telnet عن طريق فتح اكثر من Telnet, هي

← يمكن للمهاجم ان يحصل على حساب ضيف ممكن قد يكون موجودا في اي مكان داخل المجالات الموثوقة للخادم.

[2] SSH [Secure Shell] vlunerabilities

Telnet لهنفس عيوب ال

* Configuration of SSH :
  - step 1 :- Configure a user with apassword
  - step 2 :- Configure the hostname and domain name.
  - step 3 :- Generate RSA keys
  - step 4 :- Allow SSH transport on the VTy lines

∘ VTy Access Control Lists. نستطيع Telnet على Acl

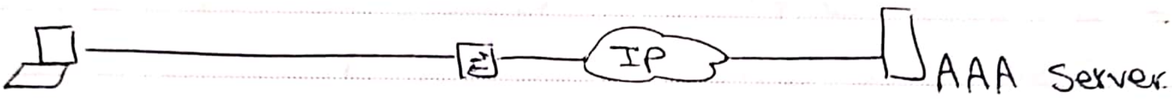
ex

```
# Line VTy 0 4
# access-list 1 per ip 10.0.0.4
# access_class 1 in
```

→ HTTp secure server

- step 1 :- Configure user name and password
- step 2 :- Configure domain name
- step 3 :- Generate RSA keys
- step 4 :- Enable HTTps (ssL) server
- step 5 :- Configure HTTp Authentication
- step 6 :- Configure an access List to Limit access

* AAA Server
[Authentication - Authorization and Accounting]



- Authentication → username + password
Authorization → privilage الصلاحيات
Accounting → mointering المراقبة

→ The AAA network-security services provide the primary framework through which you setup access Control on a cisco Ios with switch. AAA is an architectural framework for Configuring a set of three Independent security functions In a Consistant (متسقة) manner (طريقة).

يوفر الحماية بثلاث وظائف.

→ Authentication provides amethod to handle:-
- User Identification
- Login and password dialog
- challenge and response
- Messaging
- Encryption

Automation

SDN → Software defined network

- Control to Configure all network devices and help them take Correct forwarding decisions with minimum amount of H/W & S/W cost

يستخدم لتسطيب اجهزة الانترنت و يساعدها لاتخاذ القرارات معتمده على اقل حد من الـ Software و Hardware

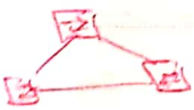
- Every router Contain SDN Controller to give Ios and Configuration file and decrease the cost

كل روتر يحتوى على Controller يعمل على اعطاءه برنامج تشغيله

← المشكله فى switches الخاصة بسيسكو انها closed system لا يمكن ان يتم تطبيق عليها اى سيستم غير الخاص بـ cisco مما يسبب صعوبه التعامل معها فى ظل التطور

→ Traditional network :

تعتمد على ٣ أشياء



- Management plane — اعطاء الاوامر
- Control plane — التحكم
- Data plane — التطبيق

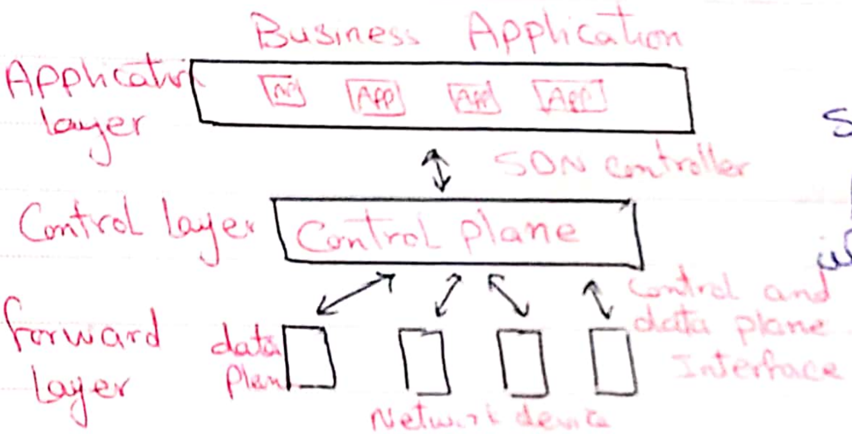
← مثلاً اذا كنت تريد تطبيق ospf على مجموعة روترات ستحتاج الى تسطيبها على كل جهاز

. النظام الجديد SDN Controller سيكون اعطاءه الامر وهو يتولى تطبيقه على كل الاجهزه

→ SDN (Software defined network)

سيقوم بفصل Control plane على جهاز خارج الشبكة
على machine ويتم التعامل مع السويتشات
ولكنها مختلفة فهي عبارة عن بورتات فقط
ستقوم بتطبيق الاوامر





هايحتوي على SDN Controller
وهو يقوم بإعداد الـ APPs
المناسبة لحل الشئ وبذلك يمكن
استخدام Software مختلف
مع الـ service (s)

→ Traditional disadvantages

1. Time Consuming — تضييع وقت في الانتظار
2. error-prone — الاخطاء البشرية
3. High Conversions — السرعة
4. Limits Automation
5. Limits Inovation — الابتكار محدود

→ SDN disadvantages

1. single point of failure
2. Single point of attack

عبارة عن Controller اذا تم العطل عليه وقفت الشبكة وحله هو عمل Controllers احتياطية

* SDN Benefits:-

1. Response to link or node failure is faster
2. Loop Avoidance is simpler
3. Management is simpler
4. Less time Consuming
5. Save Memory
6. Support Automation
7. Support Inovation ابتكار
8. Agility مرونة

** NTP → [Network time protocol]

It is an application using UDP port 123 adjust network device time & date

بروتوكول بيستخدم لضبط الوقت والتاريخ

** Syslog → It is Application using UDP used to make devices send notification about network devices changes.

تطبيق يستخدم لجعل الاجهزه ترسل اشعارات بأى تغييرات .

* NTFS → [New Technology file system]

هو افضل نظام للتعامل مع البيانات والتحكم والوصول لها وتشفيرها ويدعم الاحجام الكبيرة

⇒ domain :-

اسم الشركة ويحتوى على clients مثل Wasla.com
ويتم تمييزه
- .gov → government حكومى
- .edu → education تعليمى
- .com → مؤسسة تهدف للربح
- .eg → مصر
- .KSA → السعودية

System → Sam ← كل المعلومات موجودة فى ملف Sam
وهى بها كل users و passwords

← الجهاز يكون له اسم عادى ولكن عند دخوله فى domain يكون له اسم اخر
[Bios name] PC1 ⟶ pc1.wasla.com [host name]

⇒ domain Controller :-

هو التحكم فى domain ويكون هناك واحد primary وواحد Additional domain Controller يعمل عند حدوث عطل فى primary

⇒ Active directory :-

عبارة عن data base تحتوى على كل resources وتعطى permissions لكل clients
شروط عمل Active directory

1. Static Ip
2. Check the server name
3. You must be an adminstrator

الموضوع   التاريخ: / /

* WDS Server & WSUS Server :-

- WDS = [windows deployment service]

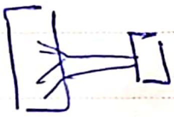
خدمه ل help desk بيقدر من خلالها يوصل لجميع الاجهزه وعملها نسخه

- WSUS = [windows server update service]

خدمه السيرفر بيصل بها الى Microsoft و يقوم بتنزيل التحديثات للاجهزه

* PBX & PRI

- PBX = [Private Branch exchange]


PBX

- خدمة توصيل المكالمات = سنترال يقوم بتوصيل كل الخطوط الموجودة في الشركة وإخرجها على هيئة وصله واحده للسنترال الرئيسي
- يقوم بدمج كل التليفونات Ip phone وتوصيلها بـ RJ-45

وكل تليفون له Ip و يستطيع نقل Voice و data عن طريق VoIp

VoIp = Voice over Ip

- PRI = [Primary rate Interface]

خط رقمي يحمل ٣٠ اتصال وهو يسمح للمؤسسات للاتصال

** CRM = [Customer Relation Management]

ادارة علاقة العميل وهو ملف excel يحتوى على جميع بيانات العميل

** Asterisk

خادم VoIP مفتوح open source يتم استخدامه لتكوين الاتصالات باستخدام VoIP

** IVR = [Interactive voice response]

نظام الرد على العميل

→ Single level IVR   □ → Sales / HR

– Multi level IVR   □ → English → Sales ; French → sales

* cloud   متجر لبيع الخدمات الالكترونية

1 Software as a service [SAAS]

تأجير Software كخدمة مثل Gmail وهذا يعمل على التوفير ولا يحتاج لتسطيب او Management

2 Platform as a service [PAAS]

بيئة عمل متكاملة يستخدمها المبرمجون ولكن لا يمكنهم التحكم بها

3 Infrastructure as a service [IAAS]

بنية تحتية [هارد - رامات - .....] يستخدمها server domain

ومميزاته انه يمكن التحكم في server ولكن يحتاج الى security

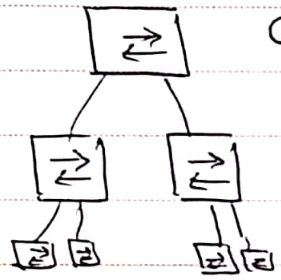
⇒ System 32 :-   windows/system 32

فولدر داخل windows يتواجد مع النسخة ويحتوى على أشياء مهمة للنظام ومعظم الفولدرات تكون exe ، ويحتوى على drivers وهو الخاص بجميع التعريفات - يصعب حذف هذا الملف منعاً لتدمير النسخة

⇒ Host file :-   windows/system32/driver/etc

هو مسار يقوم بجلب المواقع عند فتحها يكون هناك 127.0.0.1 وعند كتابة الموقع بعدها تقوم بمنعه ويستخدمه الهكر لمنع برامج الفيروسات حتى يتمكن من الاختراق

MBR [Master boot record]	GPT [Guid partition Table]
1 لا يدعم أكثر من 2TB	1 لا يدعم أكثر من 2TB
2 يدعم ٤ برتشينات فقط 4 primary partition	2 يدعم ١٢٨ برتيشن 128 primary partition
3 تخزين البيانات مرة واحدة فقط حيث انه لا يقوم بعملية نسخ احتياطي	3 يخزن المعلومات في أي وقت لأنه يحتوي على نسخة احتياطية لحالة حدوث تلف
4 صعب في دعم windows 8 وما فوق	4 يدعم انظمة Linux وما فوق Windows 8



• Core switch :-

هو السويتش الذي يخرج من LAN الى WAN ويوفر نقطة التجميع النهائية

• Distribution switch :- التوزيع

- هو السويتش الذي يوصل بين Core switch و Access switch ومهمته توصيل الكابلات لـ VLANS المطلوبة

- يحمل 15 Giga switch كسويتش توزيع

• Access switch التوصيل

المسئول عن توصيل الاجهزة بالشبكة وبه الكثير من الـ Ports و Giga ethernet هي الأكثر استخداماً.